



Hands-on AWS in 3 Weeks

-Chad Smith



Account Creation and Login

Account Creation

<https://portal.aws.amazon.com/billing/signup#/start>



Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.



Sign up for AWS

Email address

You will use this email address to sign in to your new AWS account.

Password

Confirm password

AWS account name

Choose a name for your account. You can change this name in your account settings after you sign up.

Continue (step 1 of 5)

[Sign in to an existing AWS account](#)

Account Creation

<https://portal.aws.amazon.com/billing/signup#/start>



Continue (step 1 of 5)

[Sign in to an existing AWS account](#)

Root Account Email Guidance



Use a distribution list
(corporate)

Use an alias (personal)

Root account email can
only be changed by the
root user

If you close the account,
that root email cannot ever
be used again

Securing the Root Account



Sign in

☒ **Root user**

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**

User within an account that performs daily tasks. [Learn more](#)

Root user email address

username@example.com

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

— New to AWS? —

Create a new AWS account

If the sign-in page asks for an email address....

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Securing the Root Account



Sign in

☒ **Root user**

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**

User within an account that performs daily tasks. [Learn more](#)

Root user email address

username@example.com

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

— New to AWS? —

Create a new AWS account

You're using the root account, which should be reserved for specific actions

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserv

When is the Root Account Required?



Change root user details

Change AWS support plan

Activate access to the Billing
and Cost Management
Console

View billing tax invoices

Restore IAM User permissions
for only IAM administrator

Sign up for GovCloud

Close the account

When is the Root Account Required?



Configure S3 bucket for
MFA delete

Edit/Delete S3 bucket
policy with invalid VPC ID
or VPC Endpoint ID

Enable “receive billing
alerts” (***do this!***)

Demo

Log in using root account credentials

Look at dashboards for viewing outage impact

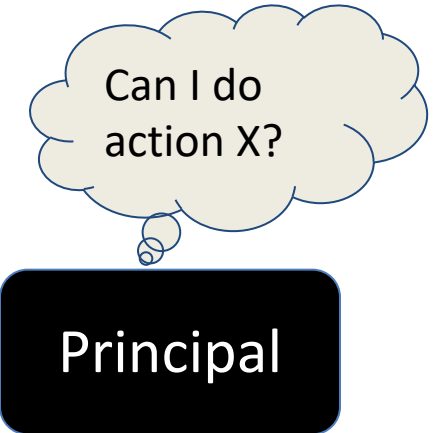
Look at the enabled regions and local zones

Opt in to billing alerts



Identity Management and IAM Permissions

AWS Permissions Evaluation

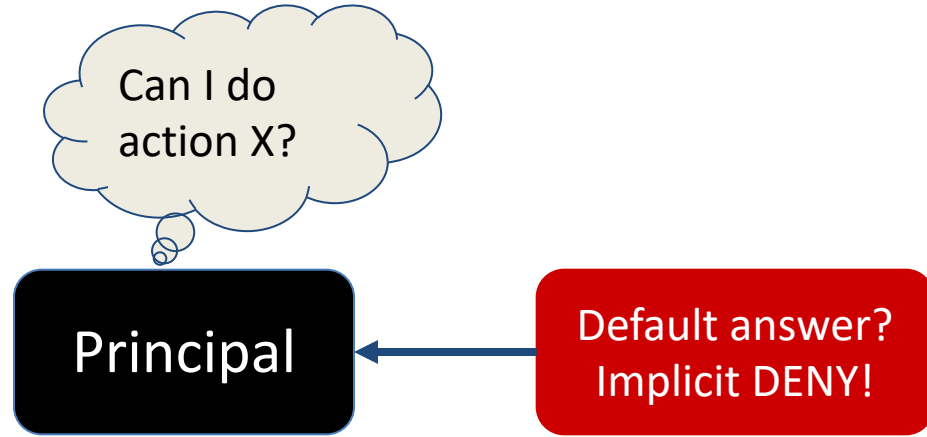


Can I do
action X?

Principal

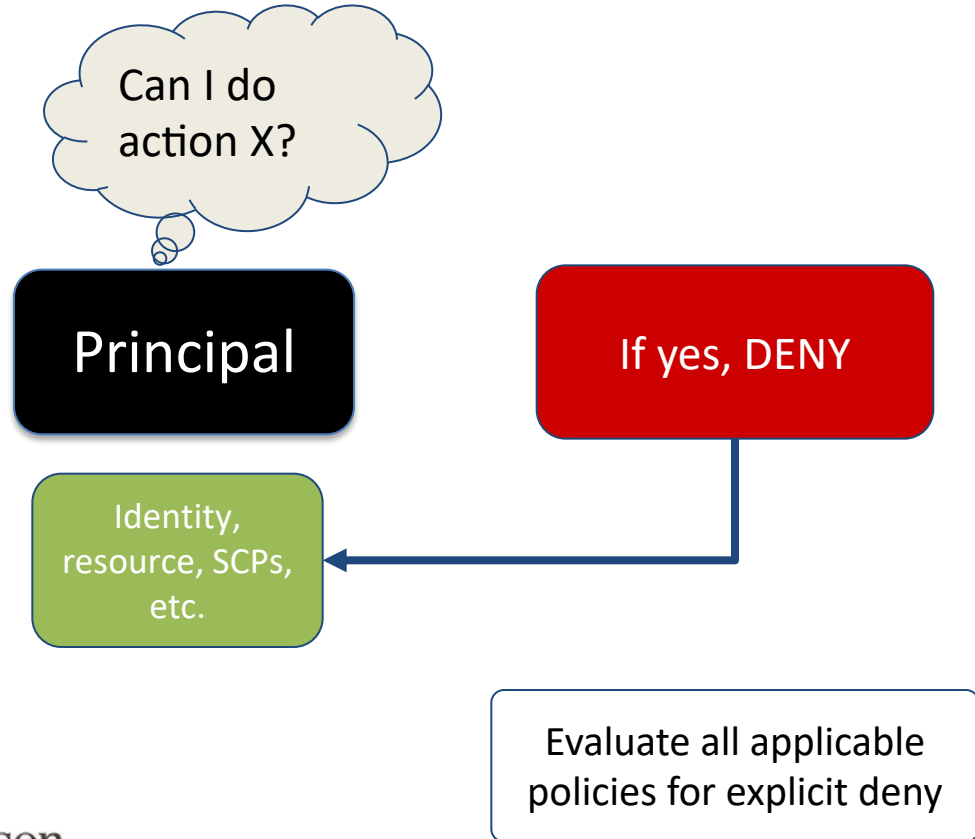
A principal can be a
user, service, role, etc.

AWS Permissions Evaluation



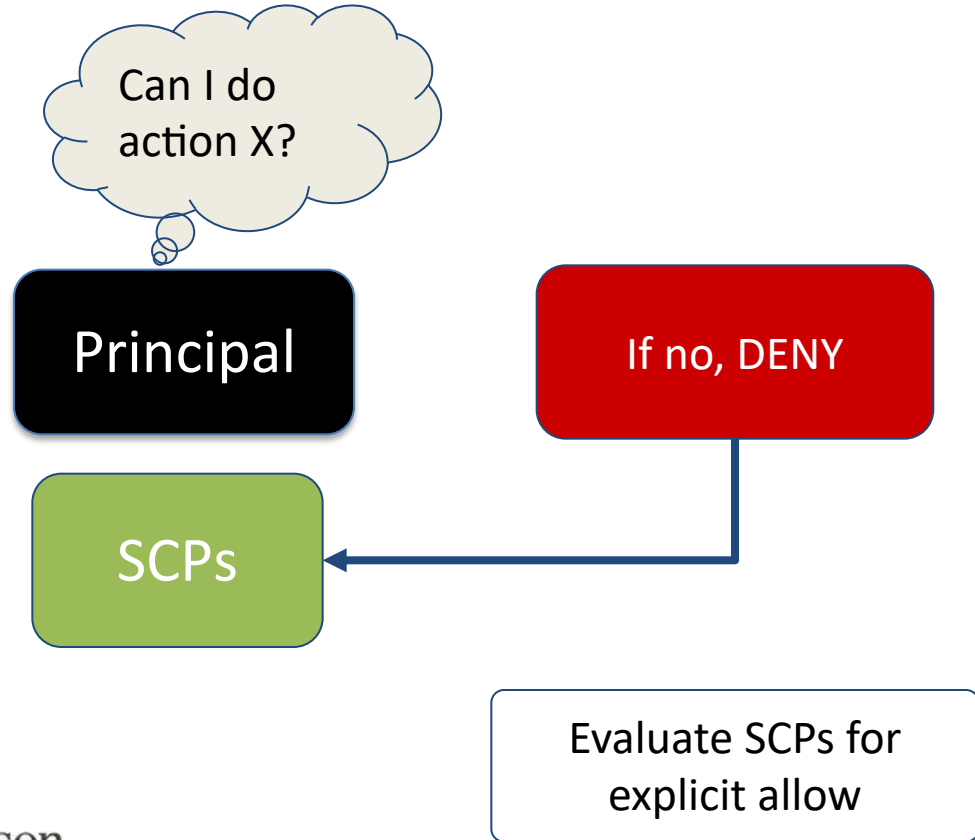
All actions in AWS have an implicit deny. There must be an explicit allow for success

AWS Permissions Evaluation



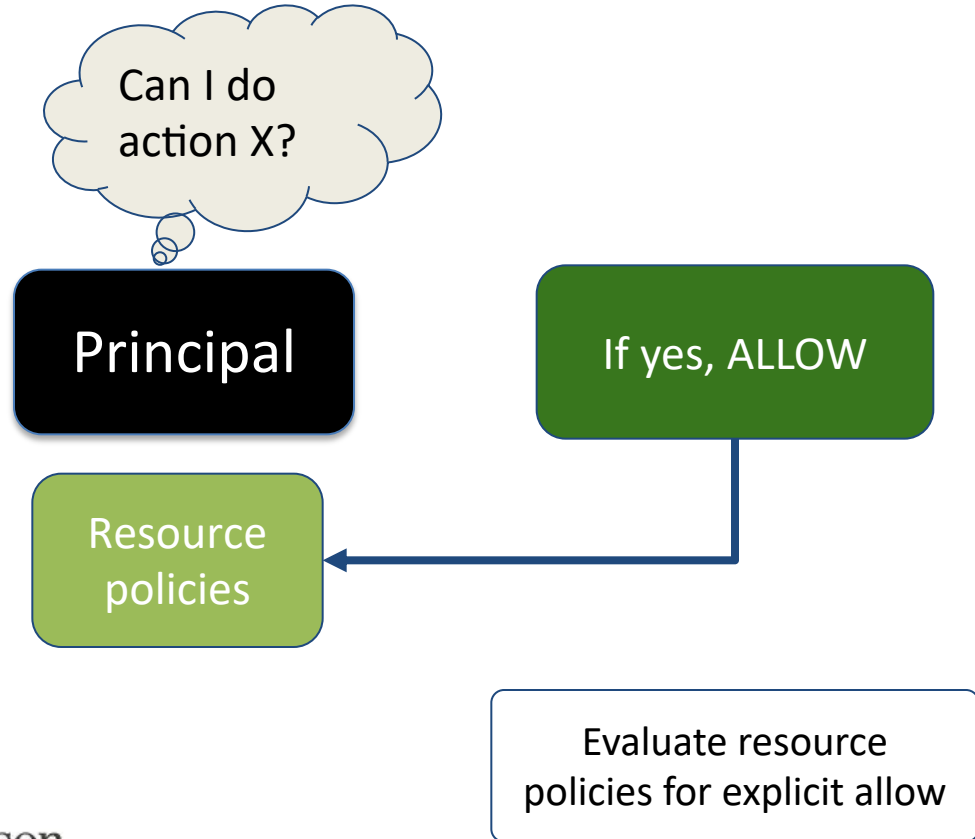
Any explicit deny takes precedence over everything else

AWS Permissions Evaluation



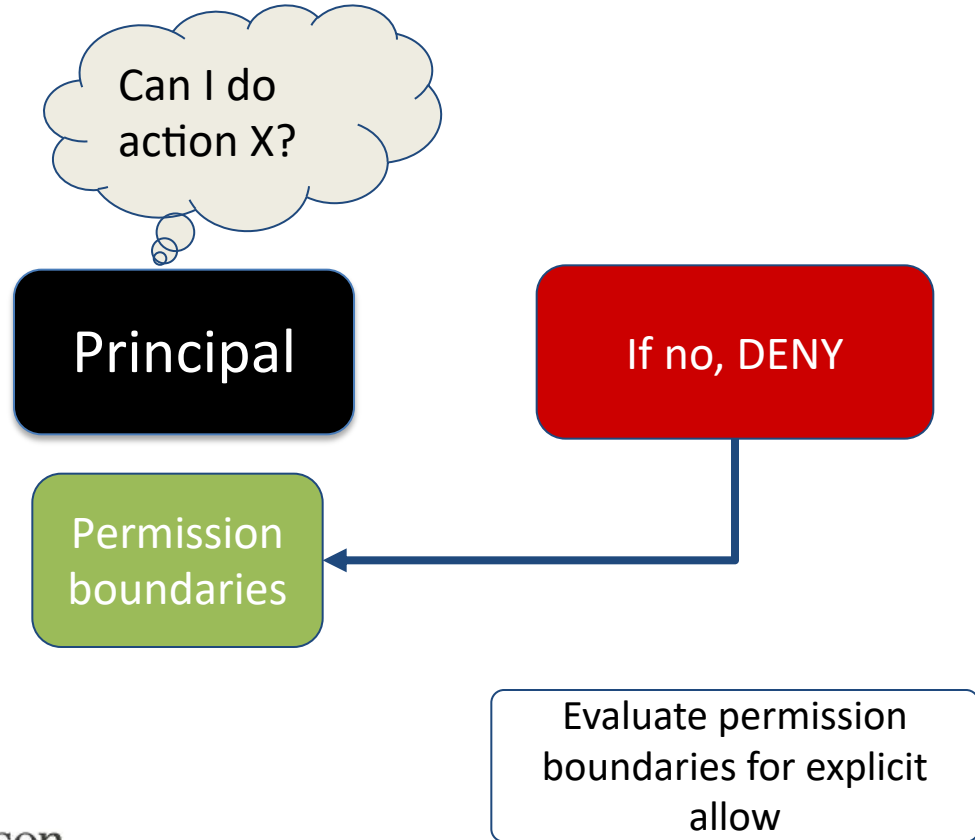
SCPs apply from the root node and each branch leading to the account

AWS Permissions Evaluation



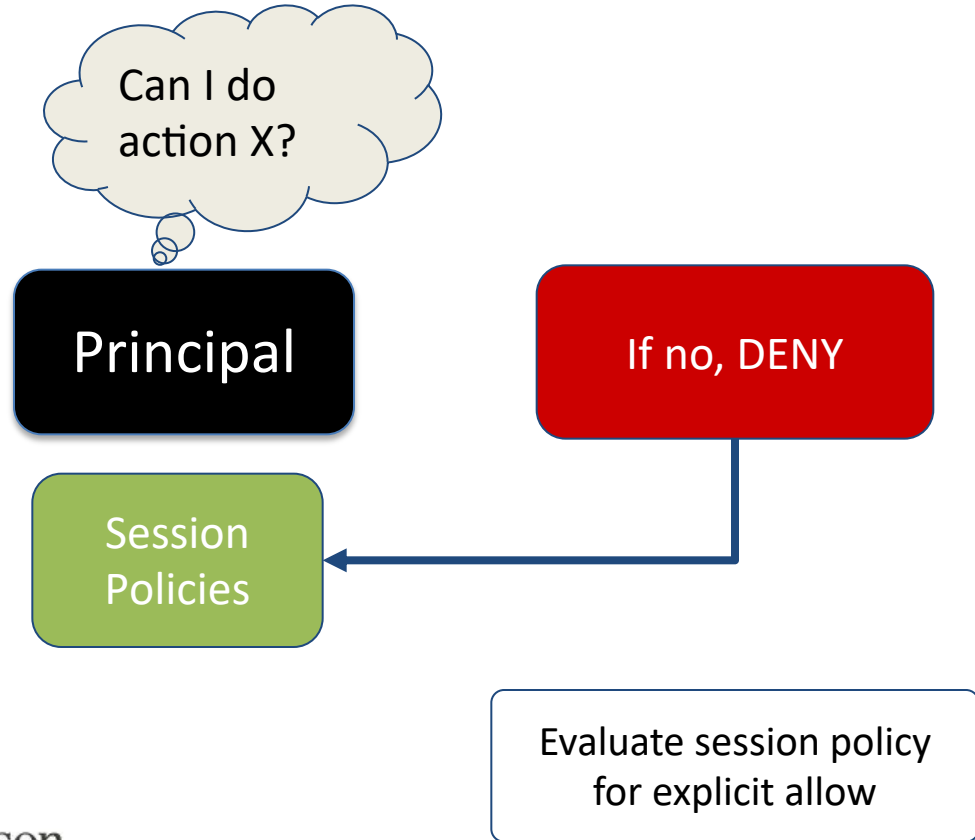
A resource policy can be more complicated if session policies involve the ARN of the principal

AWS Permissions Evaluation



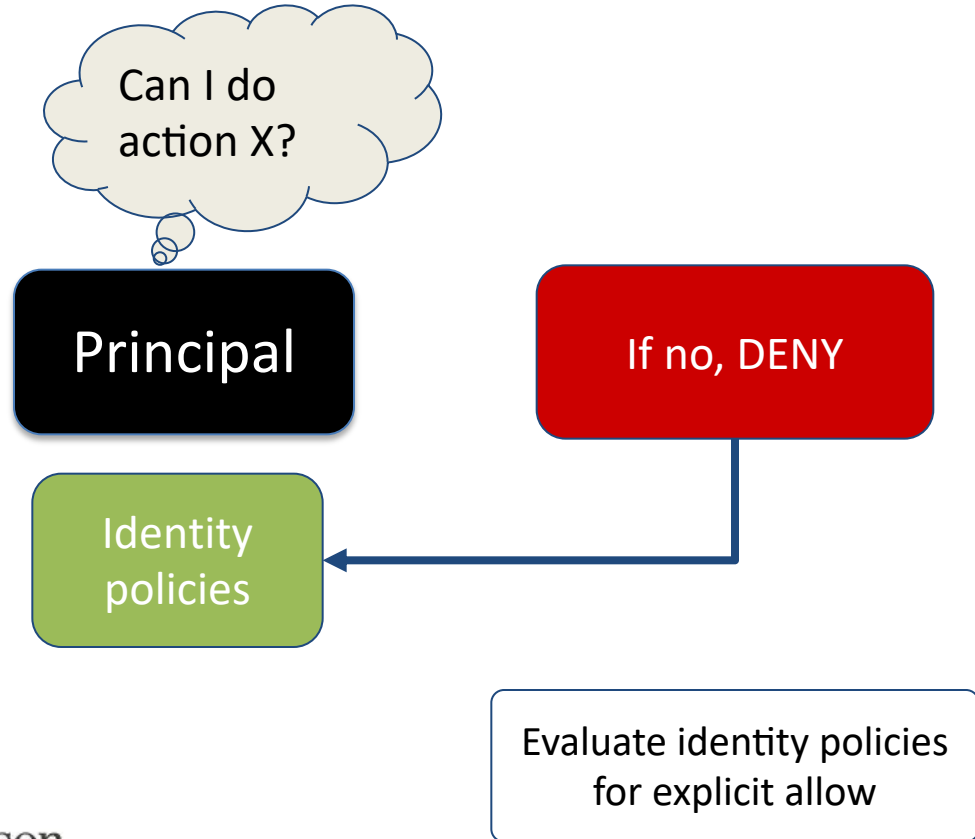
Permission boundaries can apply in multiple places

AWS Permissions Evaluation



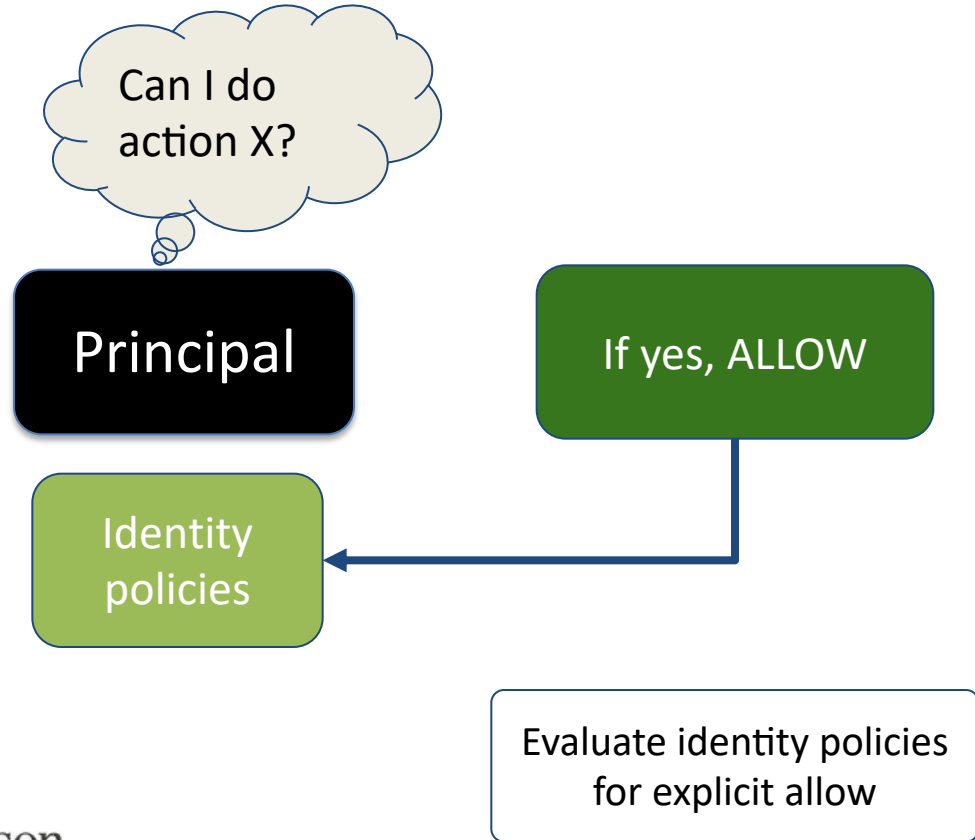
Session policies can be generic to many principals or unique to this principal

AWS Permissions Evaluation



Identity policies can include group membership or direct attachment

AWS Permissions Evaluation



As long as there is an explicit allow here, the action is allowed

IAM Resource Creation - User

Parameters



API key

OR

User/Pass



IAM Policy



IAM Group

Optional

Required

IAM Resource Creation - Group

Parameters



IAM Policy



IAM Policy



IAM Policy



IAM Policy

Optional

Required

IAM Resource Creation - Role

Parameters


Trust Policy

Optional

Required




Permissions Policy


Permissions Policy

IAM Resource Creation - Policy

Parameters

Action(s)

Optional

Required

Service(s)



Resource(s)

Condition(s)

Demo

Create IAM role for power users

Create test users

Attach policy to users for pw change

Attach policy to users for role assumption

Validate user credentials and role assumption



Account Management with Organizations

Multiple Accounts Using Organizations

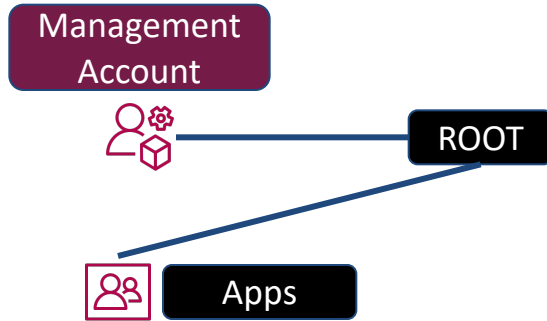
Management
Account



ROOT

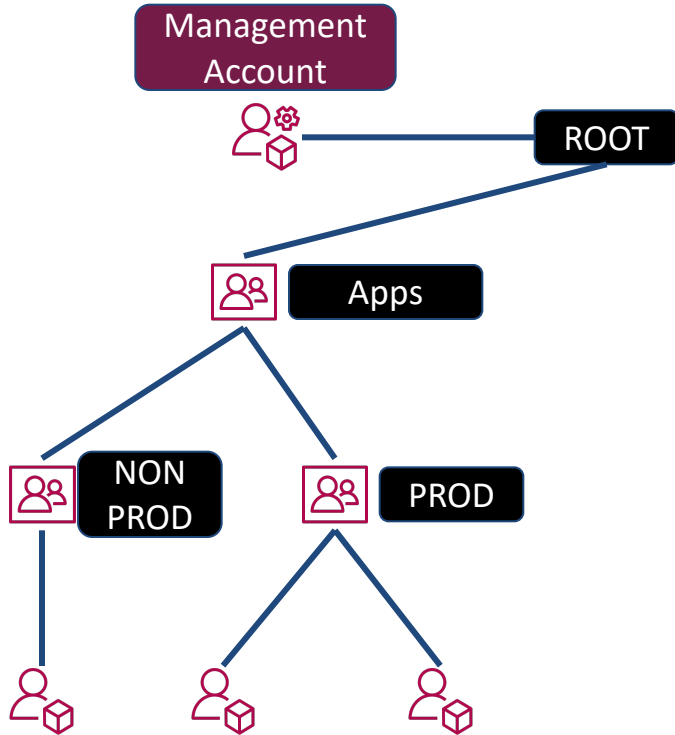
The Management
account has very
few resources
such as SSO

Multiple Accounts Using Organizations



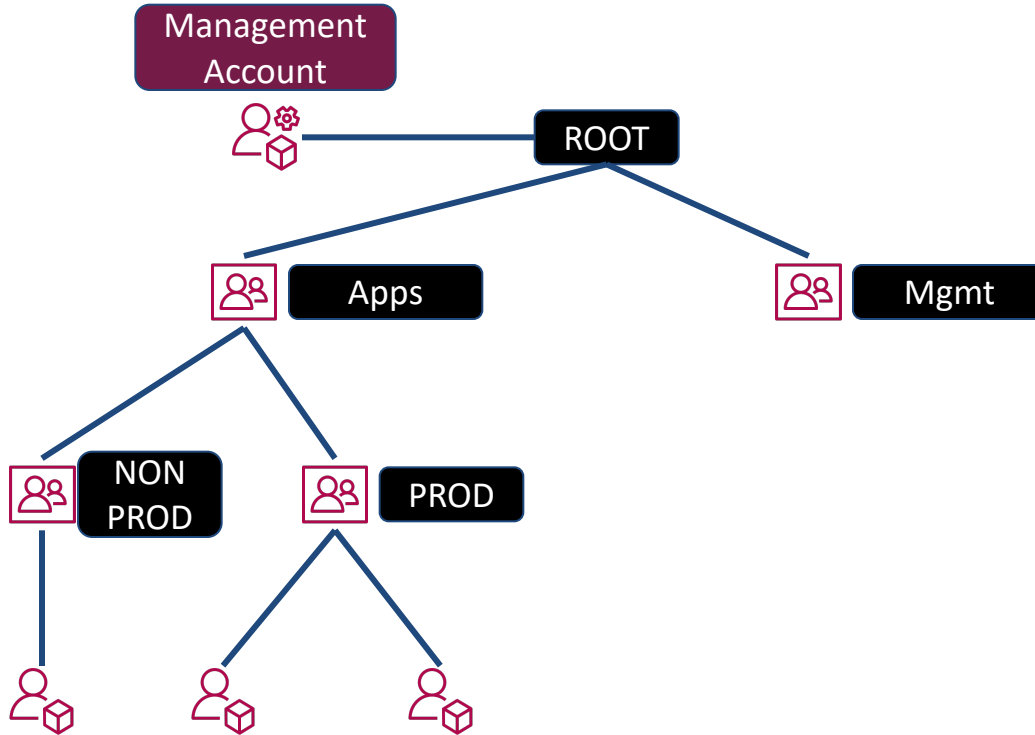
The Apps OU is
for all product
related
infrastructure

Multiple Accounts Using Organizations



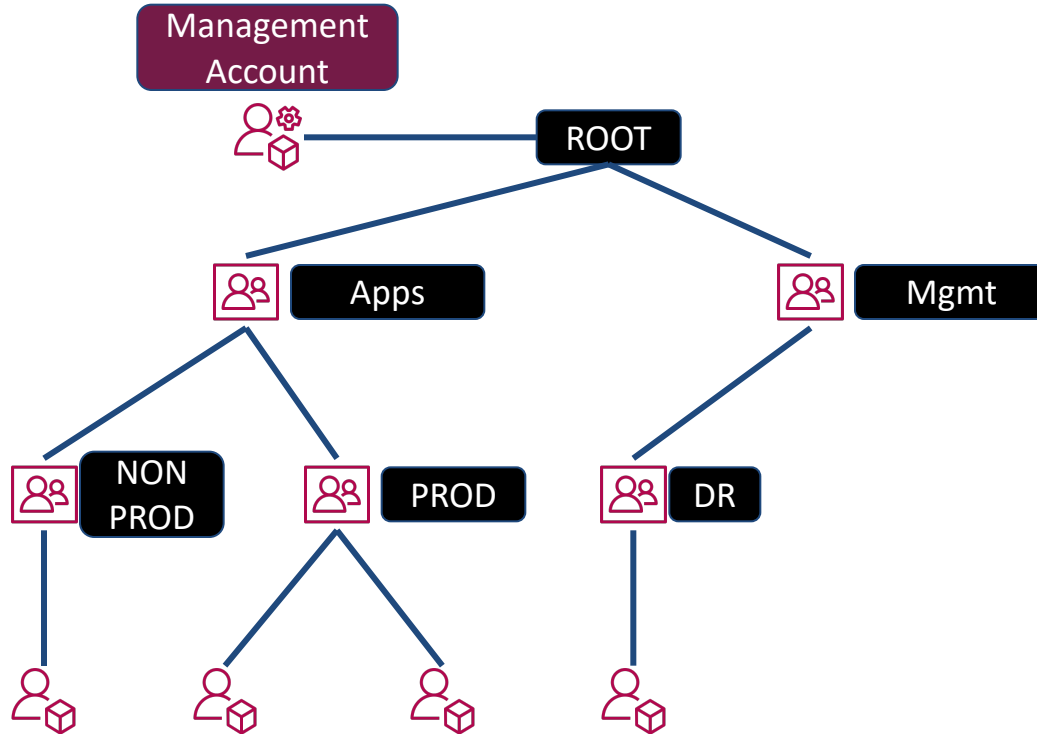
Create OUs for
Non-prod and
Prod
environments

Multiple Accounts Using Organizations



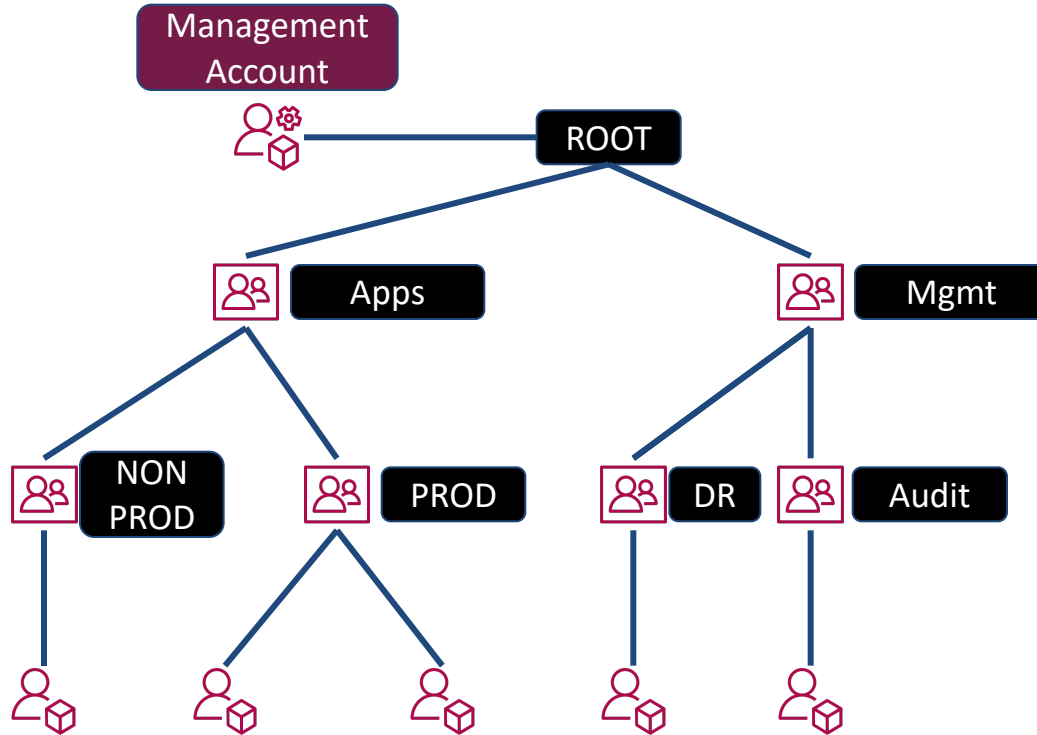
Another OU for
all management
activities

Multiple Accounts Using Organizations



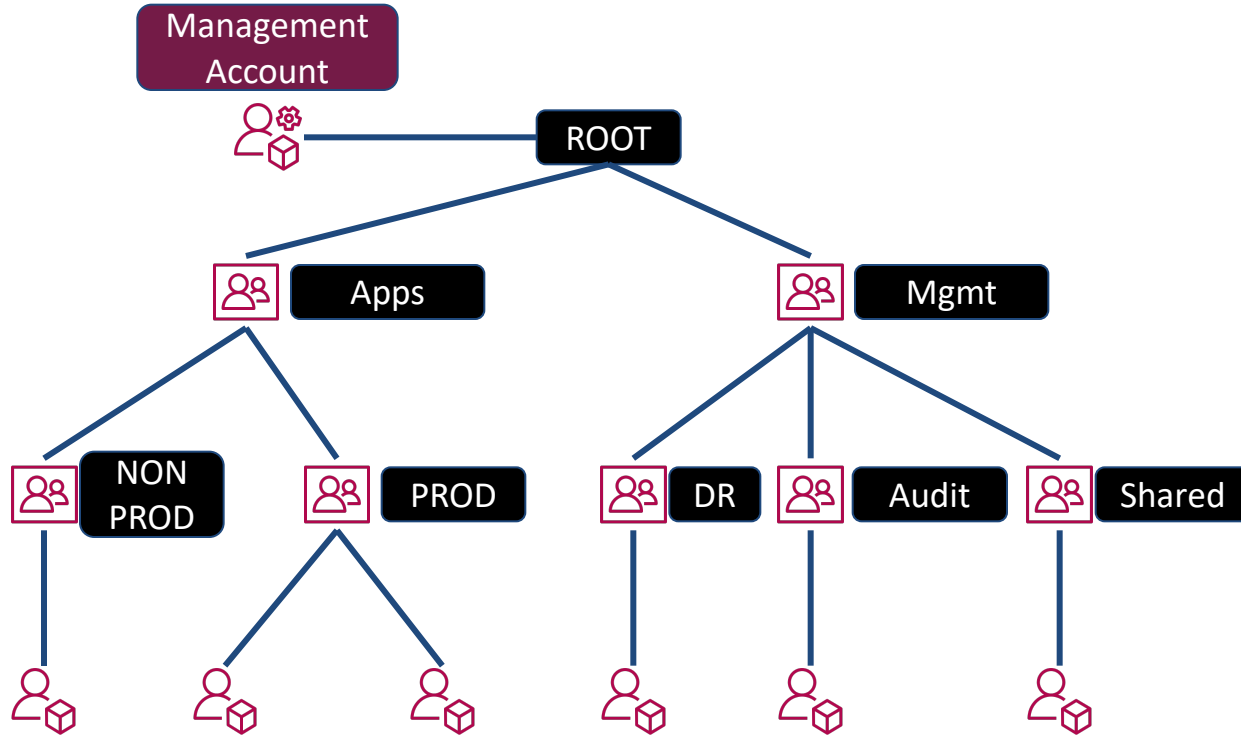
Business continuity is isolated into an OU and separate account

Multiple Accounts Using Organizations



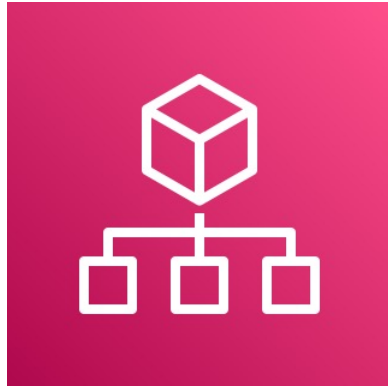
So is security and compliance auditing infrastructure

Multiple Accounts Using Organizations



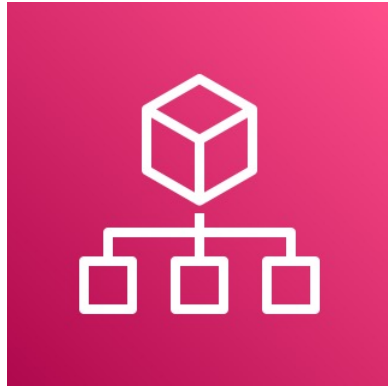
Finally, all shared resources can be placed in a separate OU and account

AWS Organizations SCPs



Service Control Policy
Supports OU structure
SCPs can allow (boundary)
SCPs can deny
Affect IAM users and roles
Affect root credentials
SCPs are inherited

SCP Exceptions



Management account

Service-linked roles

As root user:

Enterprise support registration

AWS support level change

CloudFront key changes

CloudFront trusted signer

LightSail reverse DNS

OUs and SCP Inheritance

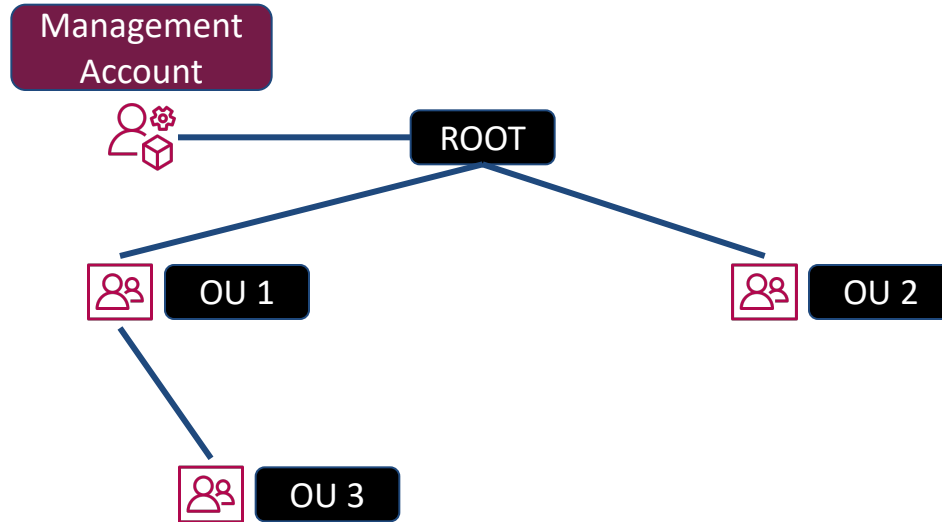
Management
Account



ROOT

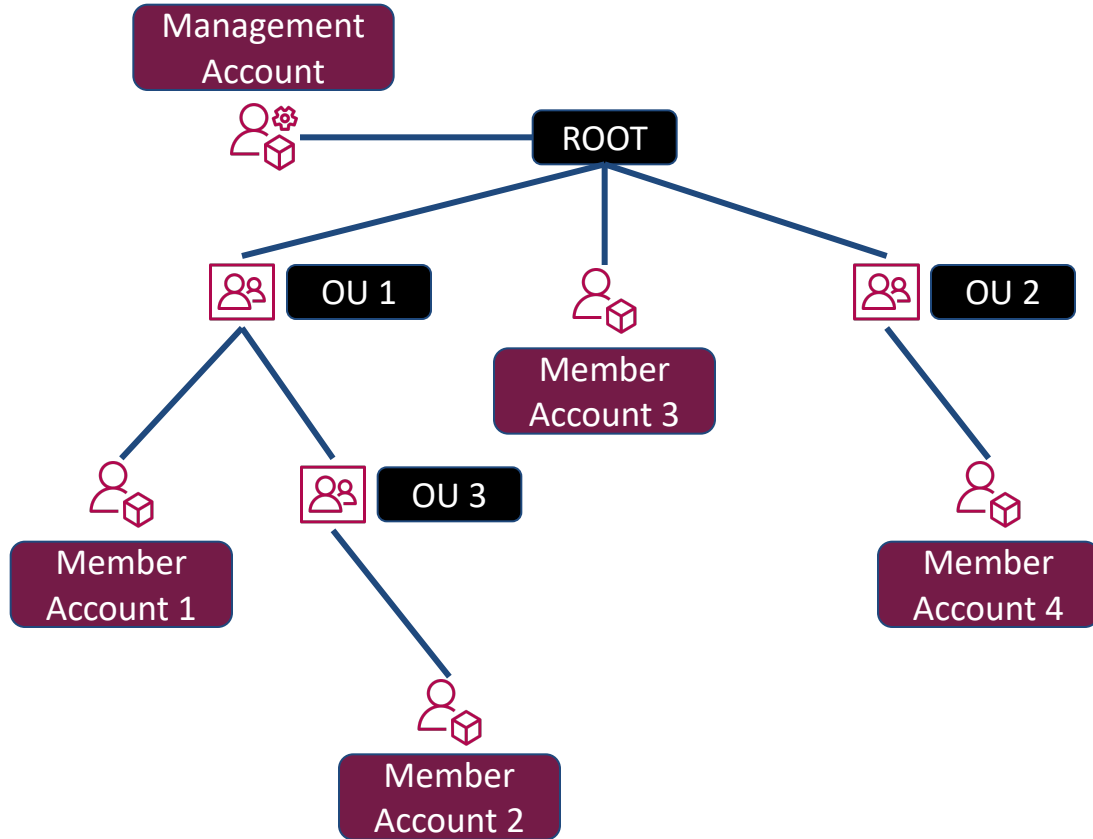
The Management account is in the OU structure but is unaffected by SCPs

OUs and SCP Inheritance



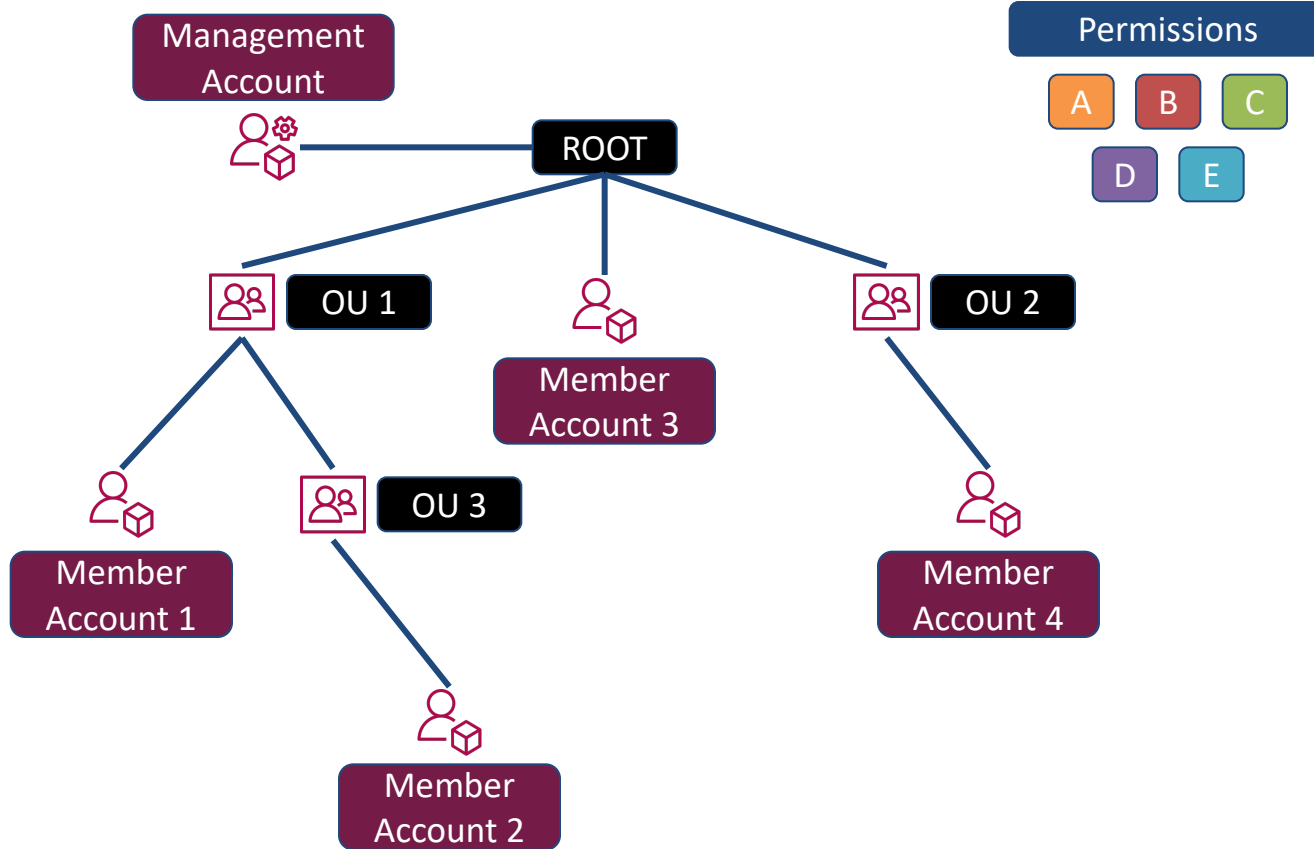
The OU structure allows nested directories (such as OU 3)

OUs and SCP Inheritance



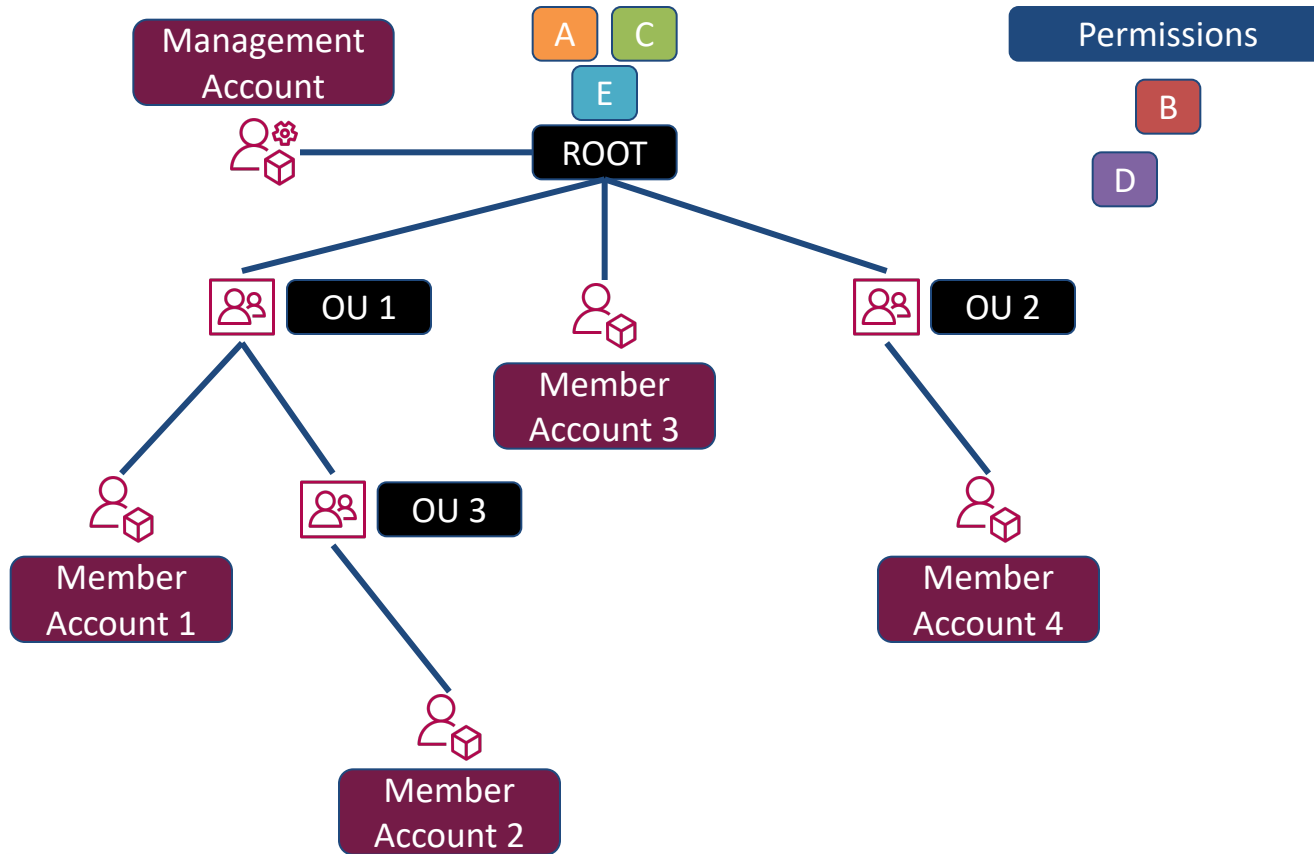
Member accounts can be placed anywhere in the structure, including under the root

OUs and SCP Inheritance



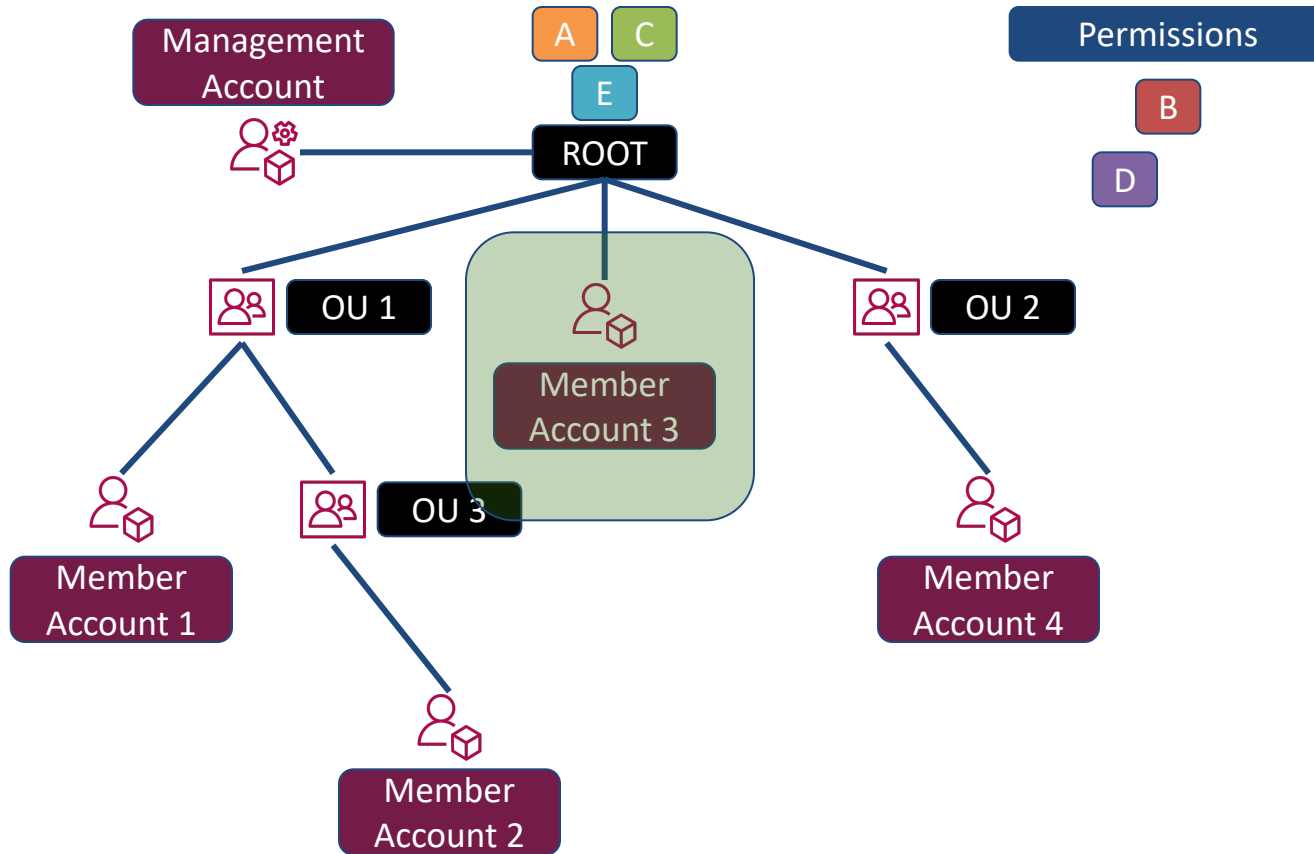
Desired permissions must be allowed at the root node to be available in any account

OUs and SCP Inheritance



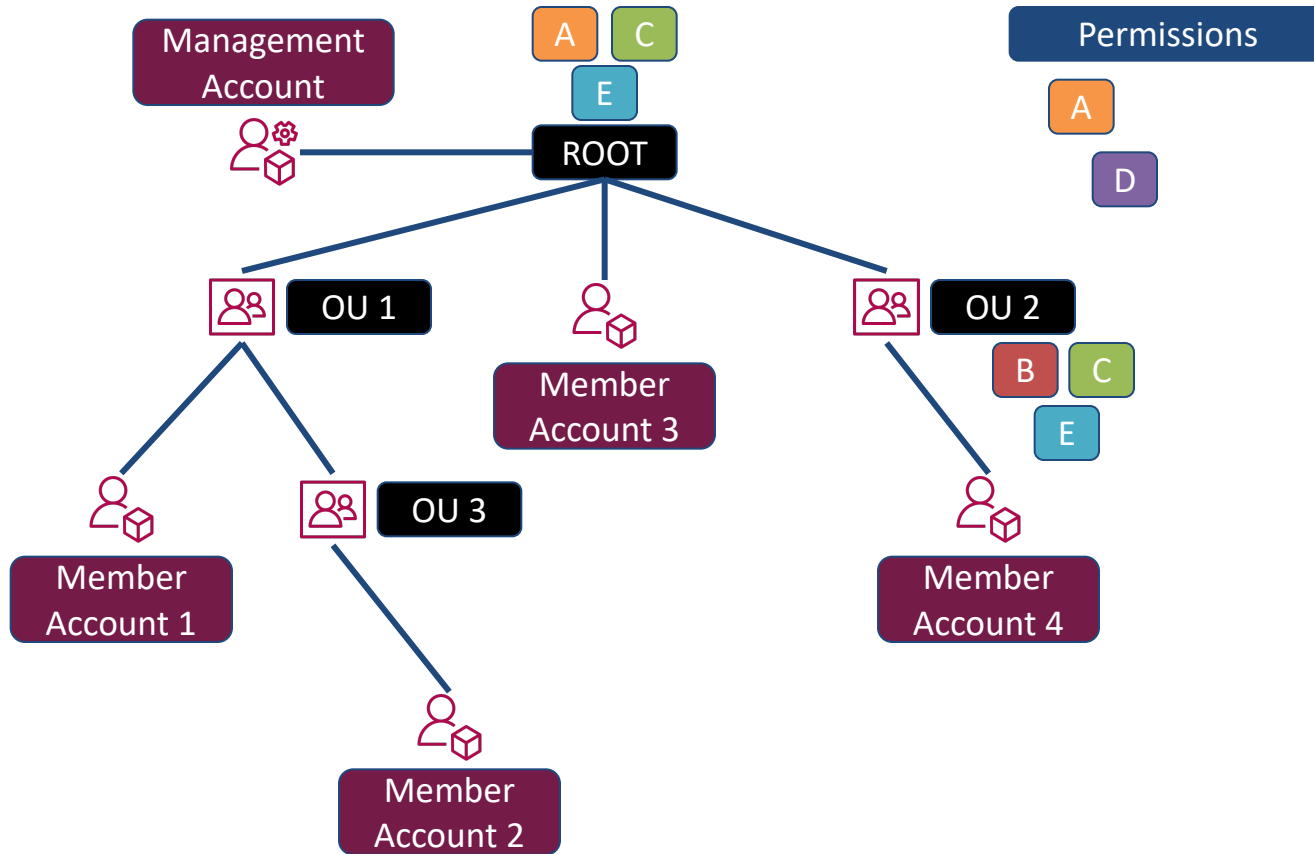
If an SCP allows
A, C and E
permissions at
the root level:

OUs and SCP Inheritance



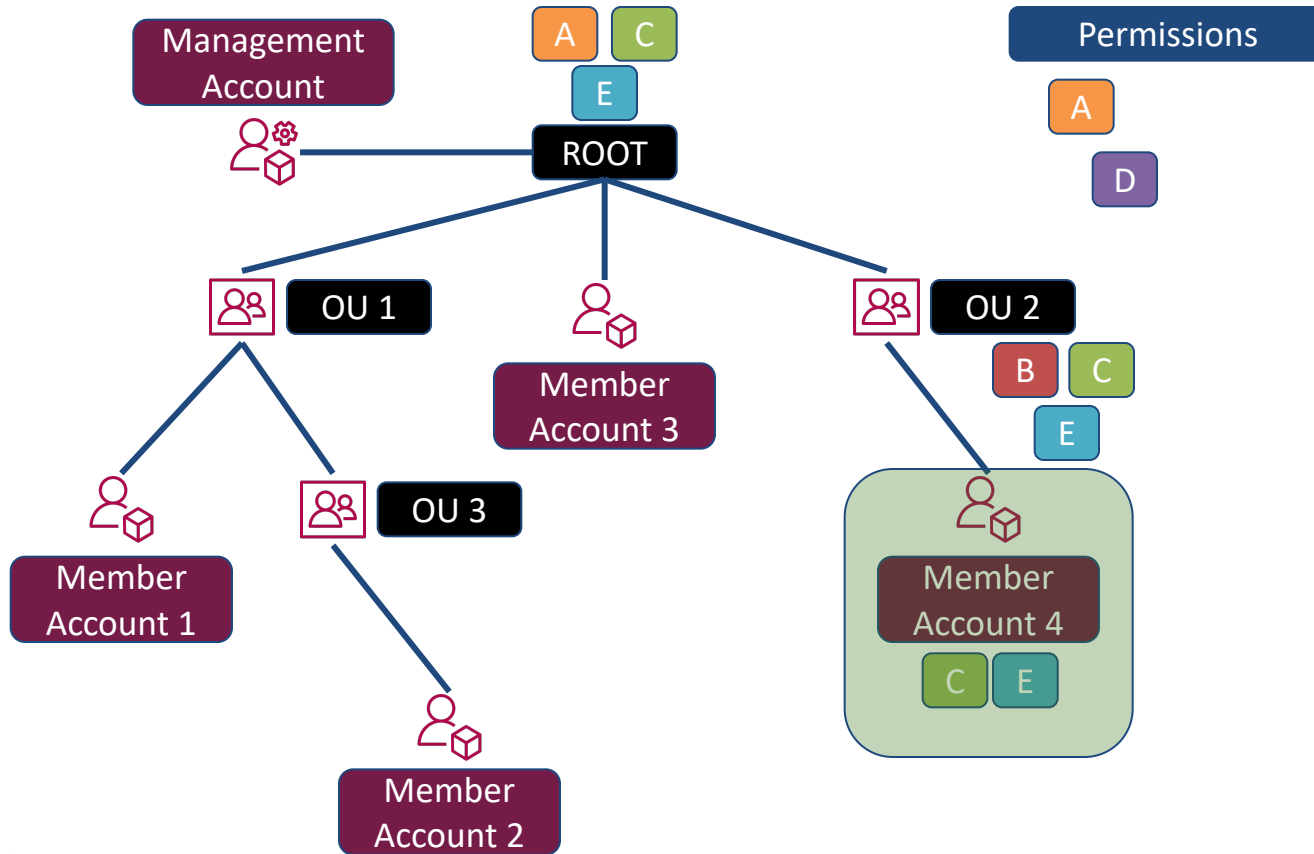
Member account
3 can use all 3
permissions

OUs and SCP Inheritance



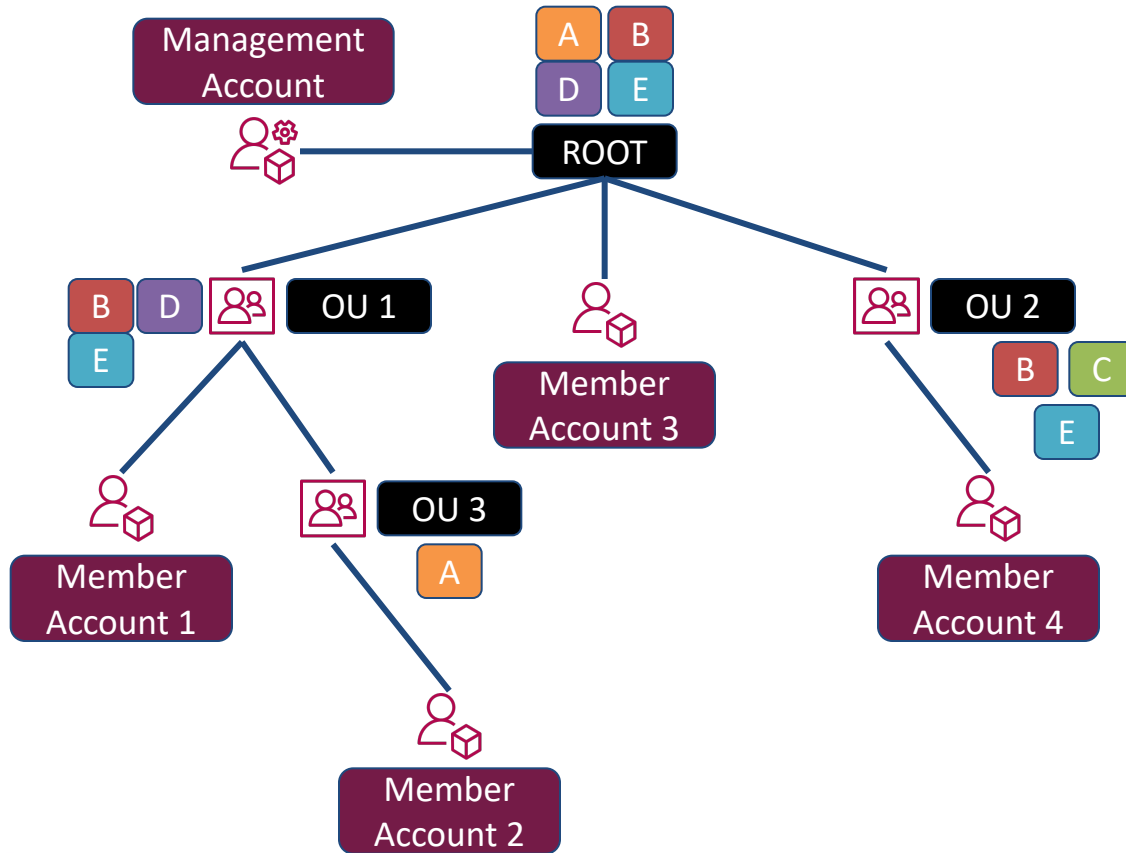
If an SCP allows B, C and E permissions at OU2:

OUs and SCP Inheritance



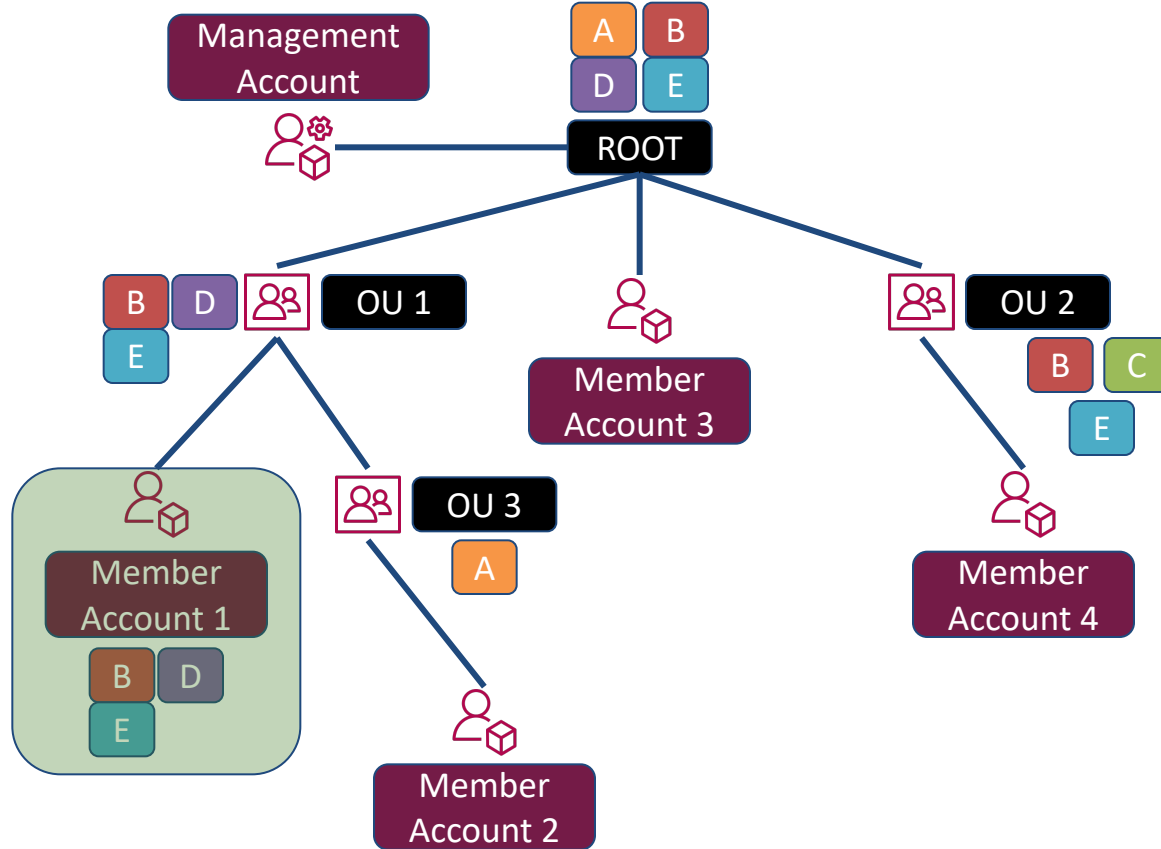
Member account 4 can use permissions C and E (the intersection of the two SCPs)

OUs and SCP Inheritance



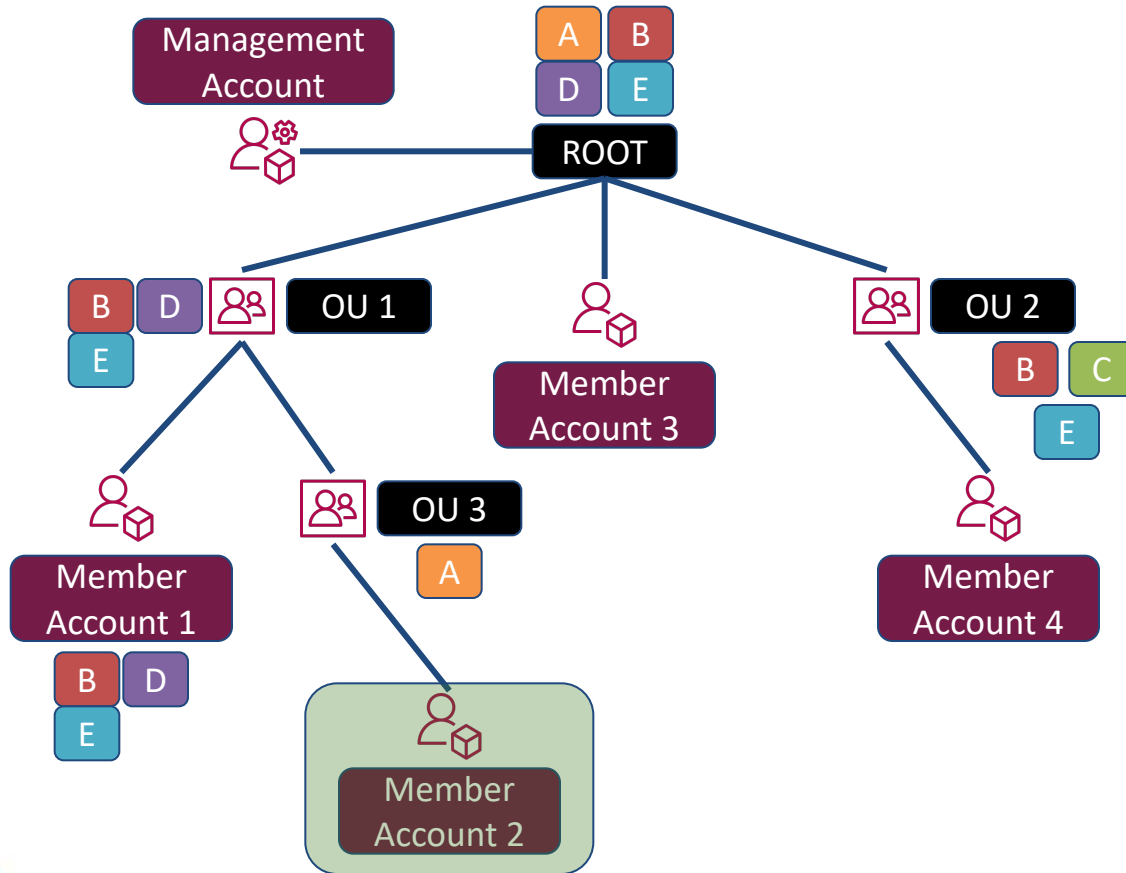
In a more complicated structure, troubleshooting can be difficult

OUs and SCP Inheritance



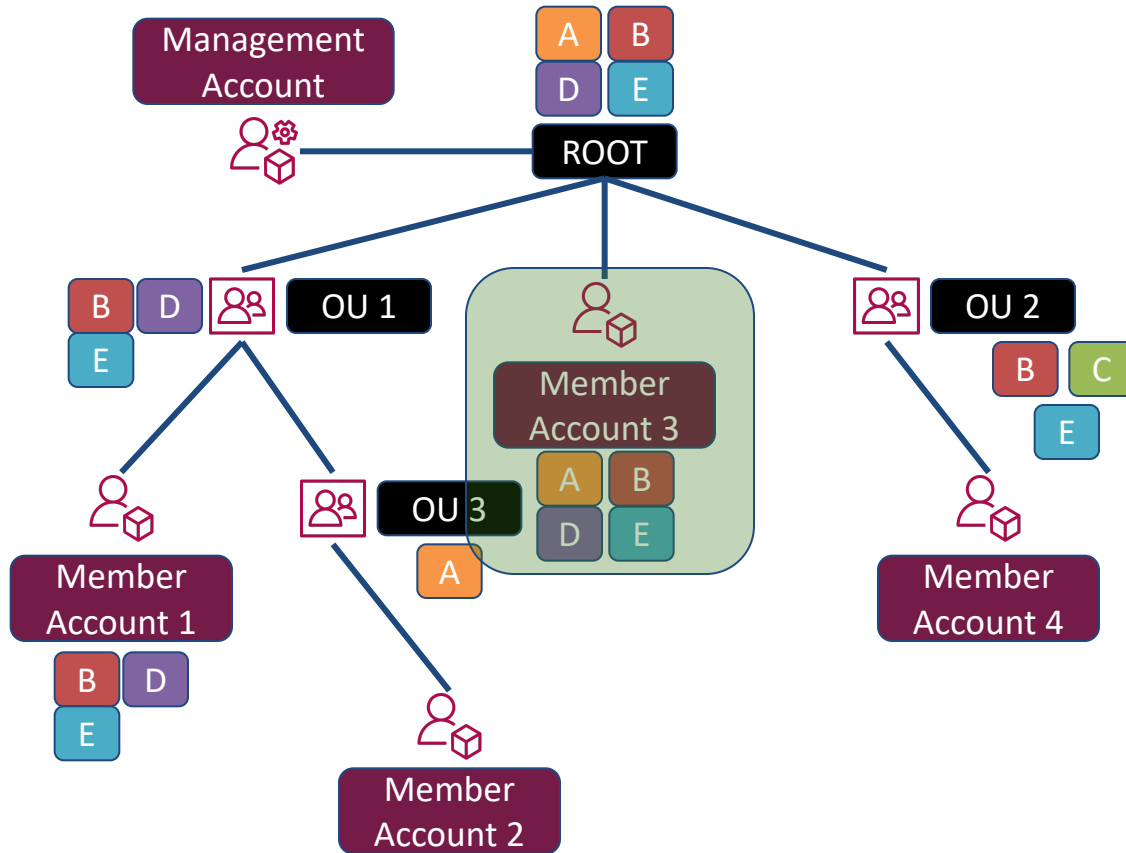
Member account 1 can use permissions B,D,E but not A because it isn't in the OU 1 SCP

OUs and SCP Inheritance



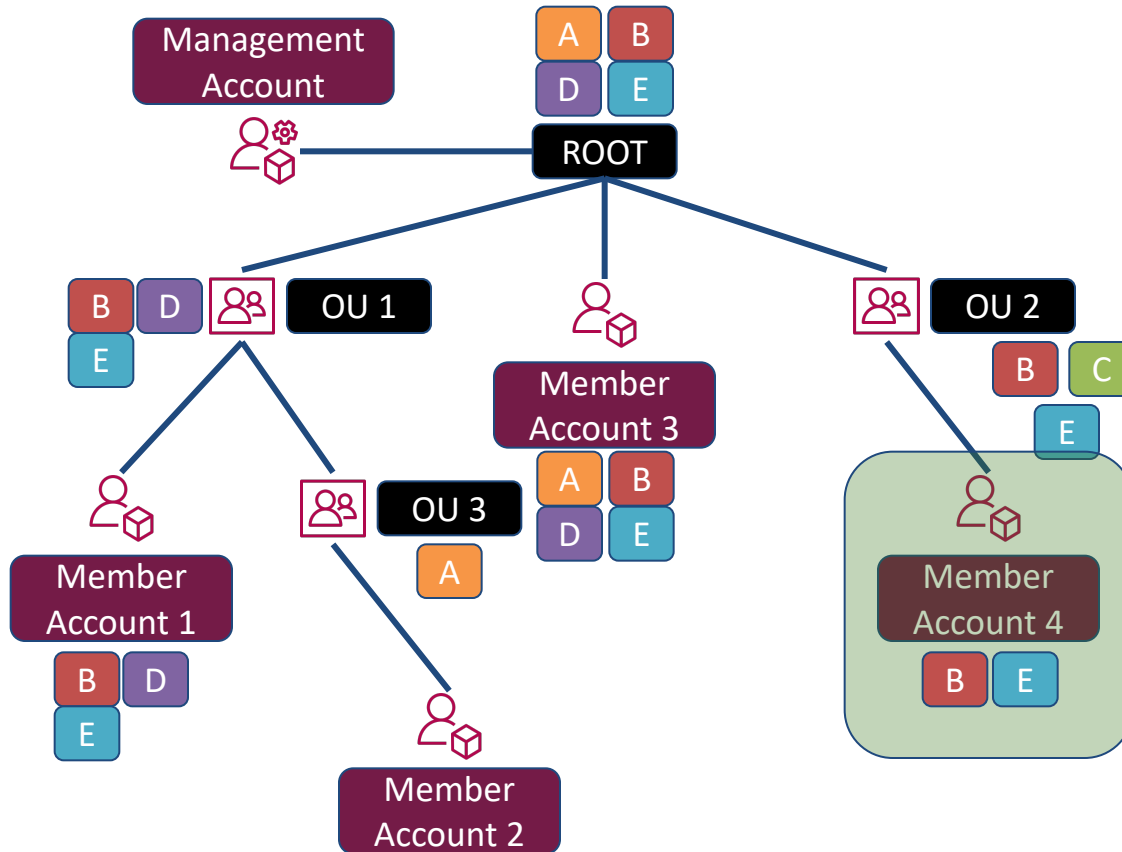
Member account 2 gets no permissions at all, which is a problem!

OUs and SCP Inheritance



Member account 3 gets A,B,D,E directly from the root

OUs and SCP Inheritance



Member account 3 gets B and E because C is not allowed at the root

Demo

Explore the Organizations dashboard
Discuss Organizations policies
Create new SCP to deny certain actions
Validate the SCP



Implementing Security Guardrails and Reports

Security Hub Basics



Central view of security alerts

Multi-account support

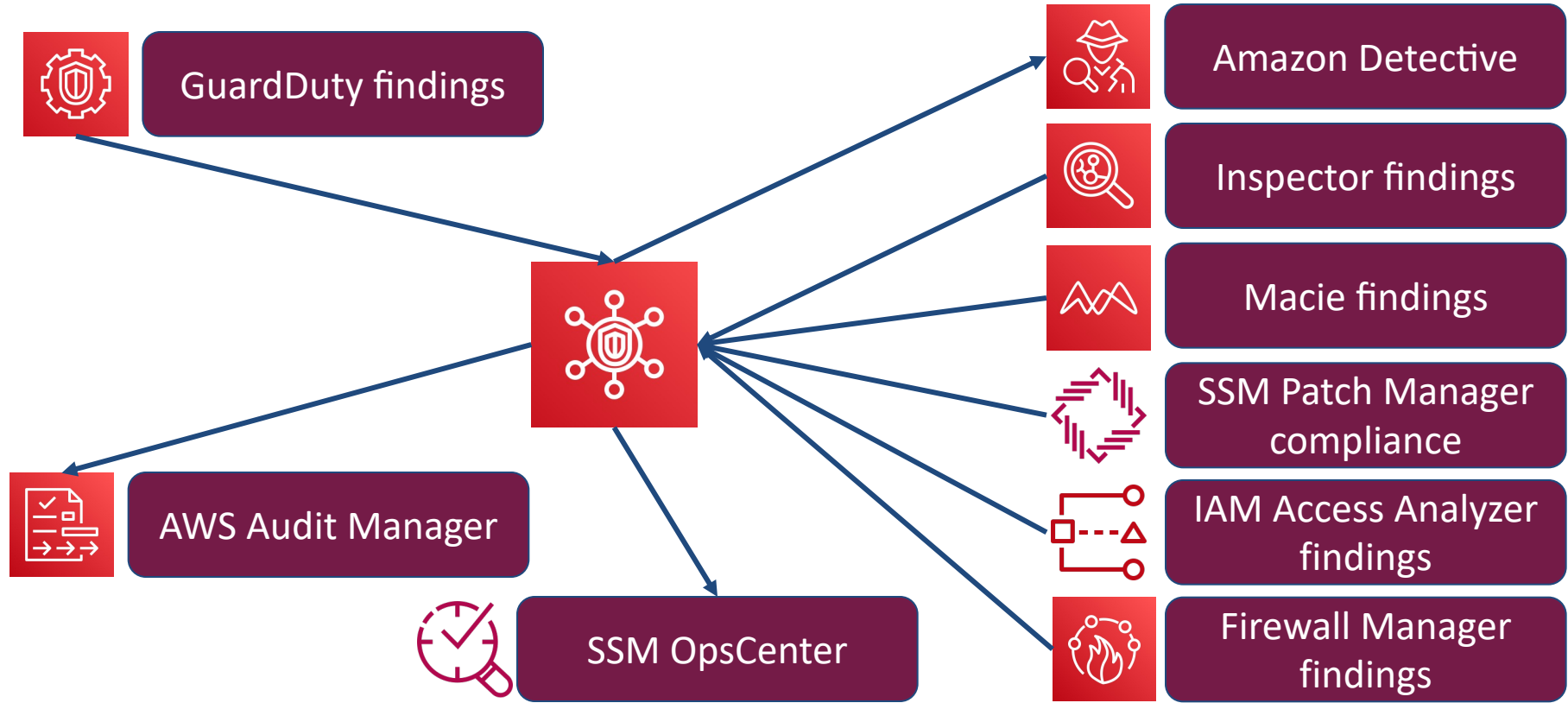
Consolidated mgmt of alerts

Alerts prioritized by severity

Automated compliance checks

External partner support

Consolidate Security Findings in AWS



Security Hub Standards



CIS AWS Foundations
Benchmark

PCI DSS Benchmark

AWS Foundational Security
Best Practices

Standardized Findings Format



Static JSON objects
Complex, inclusive
Makes analysis easier
Good reason for adoption
instead of using individual
products

Security Insights



Predefined, static
Highlight emerging trends
Discover possible issues

Demo

Explore Security Hub dashboard

Explore Audit Manager

Explore Config dashboard and compliance

Explore SSM Patch manager and compliance



Cost Allocation Tags and Budgets

Cost Allocation Tag Basics



Associate tags with billing

Enable in AWS console

Use in individual accounts

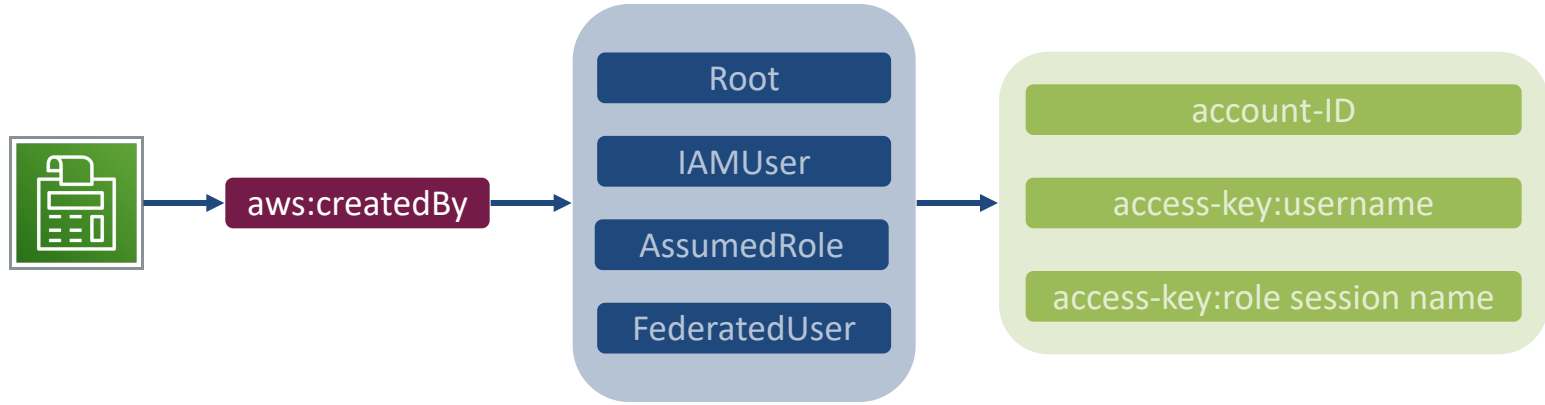
Use in management
accounts

Good reason for tag
strategy

AWS-generated tags

User-defined tags

AWS-Generated Tag Example



Only visible in Billing
& Cost Management
console and reports

Only some actions
supported

AWS-Generated Tag Support



Auto Scaling
Backup
Batch
CloudFormation
EC2
ECS
EKS
Elastic MapReduce
SSM

User-Defined Cost Allocation Tags



Use with existing tags

Use with new tags

Does not tag resources

"aws:" is reserved

Activate in Billing Console

AWS Budgets Basics



Monitor cost

Monitor utilization

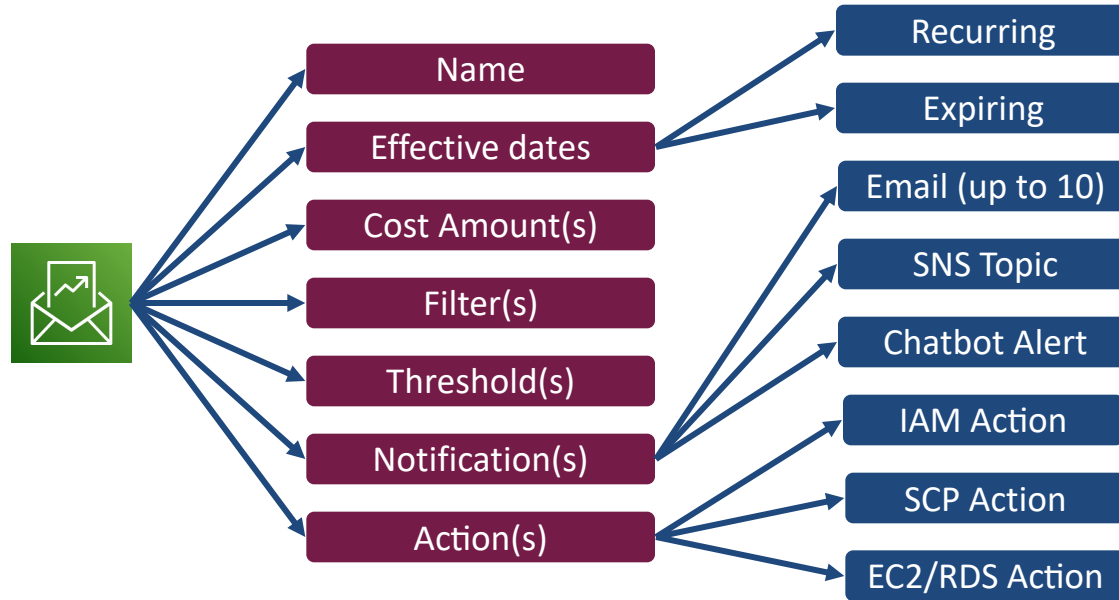
Monitor coverage

Passive notifications

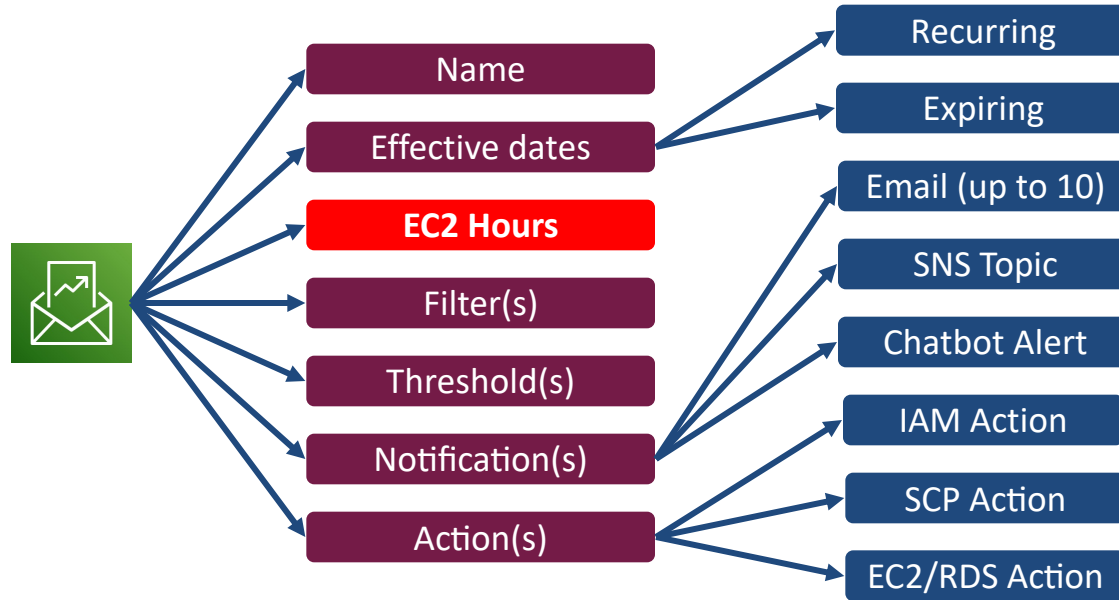
Active actions

Filters same as CE

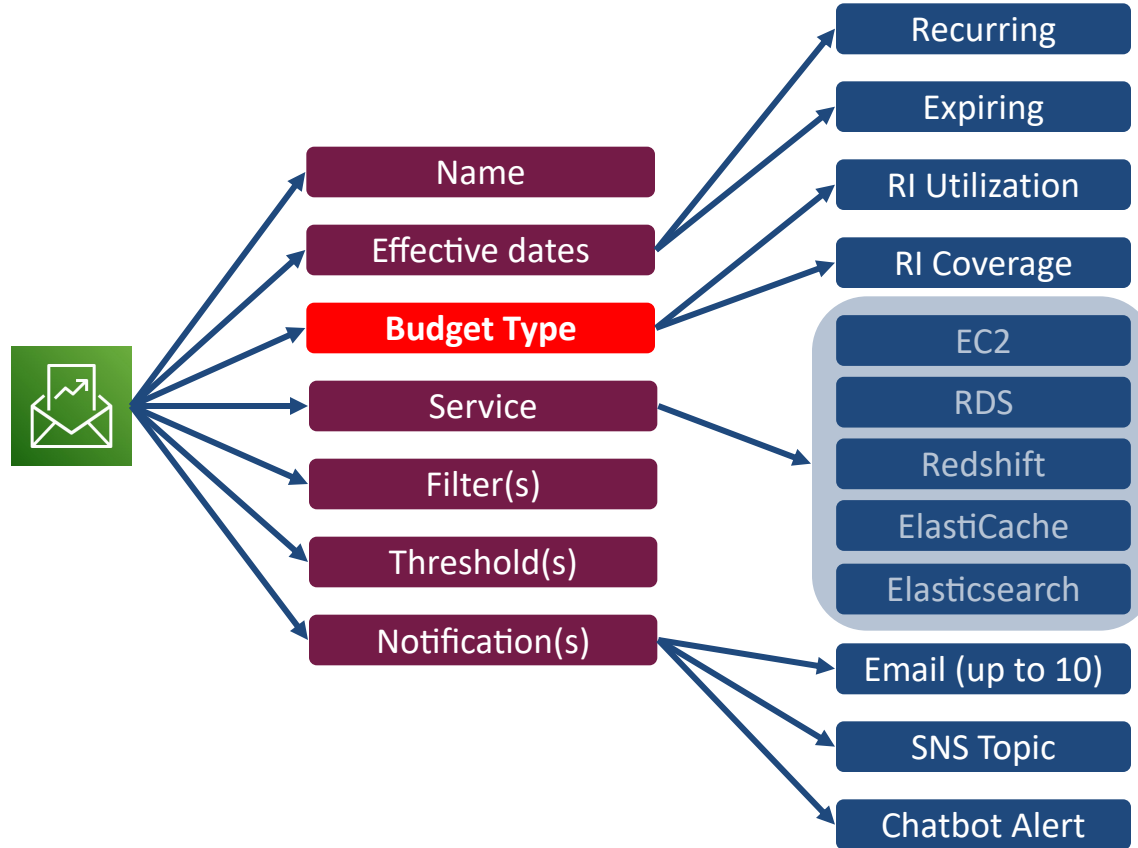
Cost Budgets



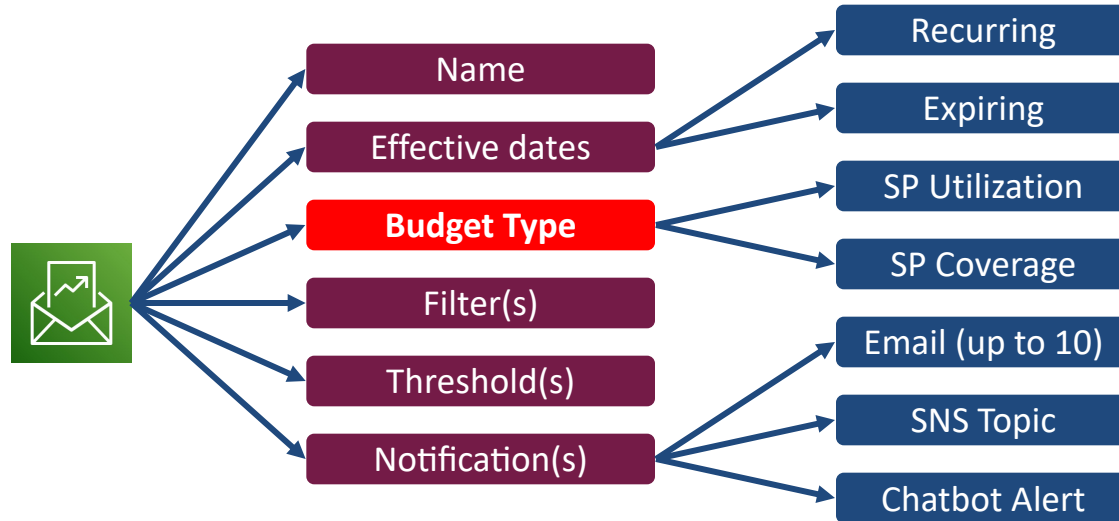
Usage Budgets



RI Utilization and Coverage Budgets



SPs Utilization and Coverage Budgets



Budget Actions



Apply IAM policy to
IAM users/groups/roles

Apply SCP to root or OU
in an Organization

Stop EC2 or RDS
instances in an account

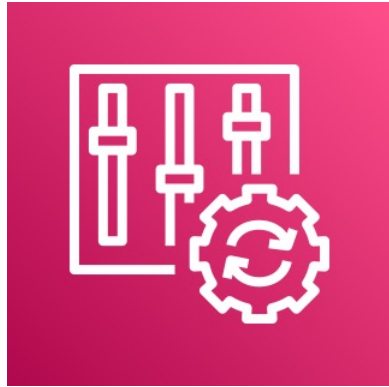
Demo

Explore Cost Allocation Tags
Create Cost Budget



Monitoring Compliance and Events

Config Basics



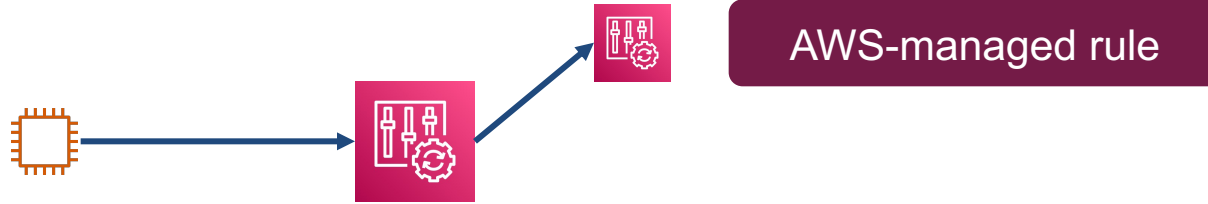
Region scope
Config Streams
Partial coverage
Capture changes
Capture config
Snapshots

Config Rule Creation Example

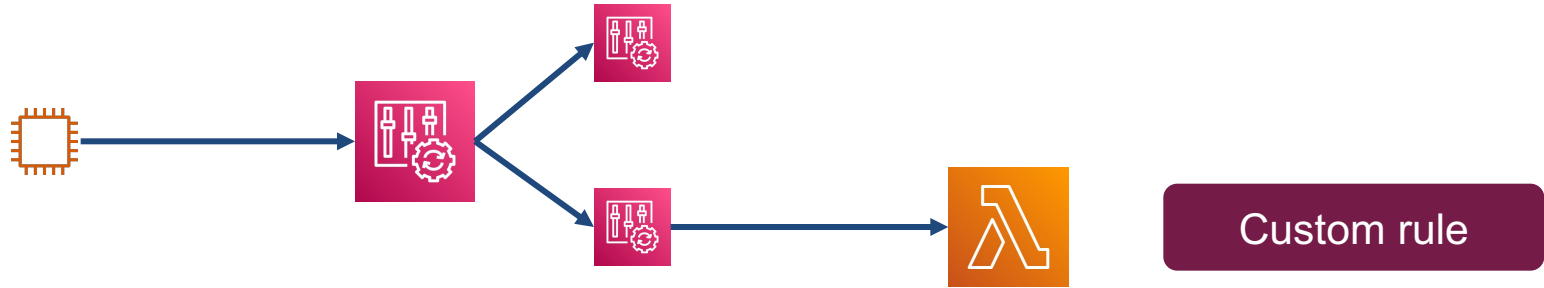


Properties and
changes for
resources

Config Rule Creation Example



Config Rule Creation Example



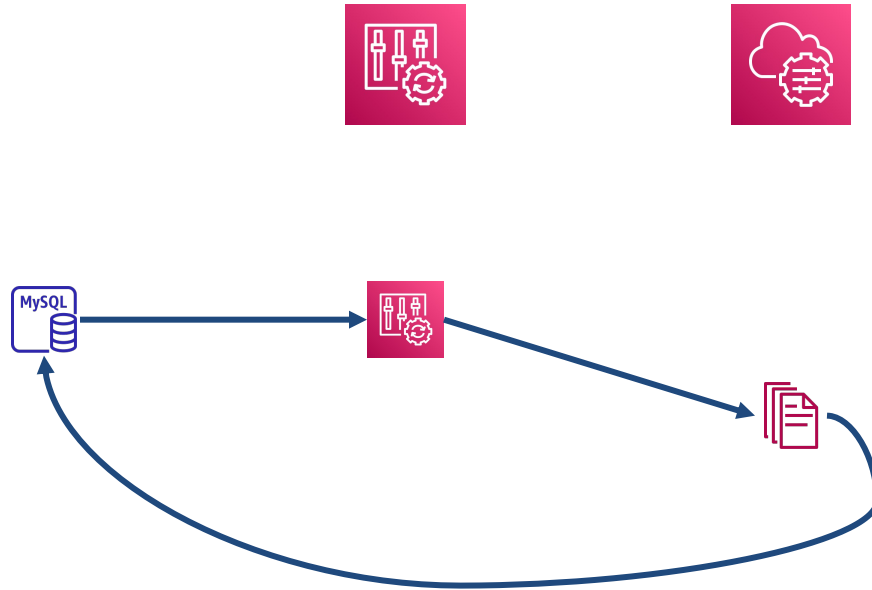
Config Rule Remediation Example

Config stream



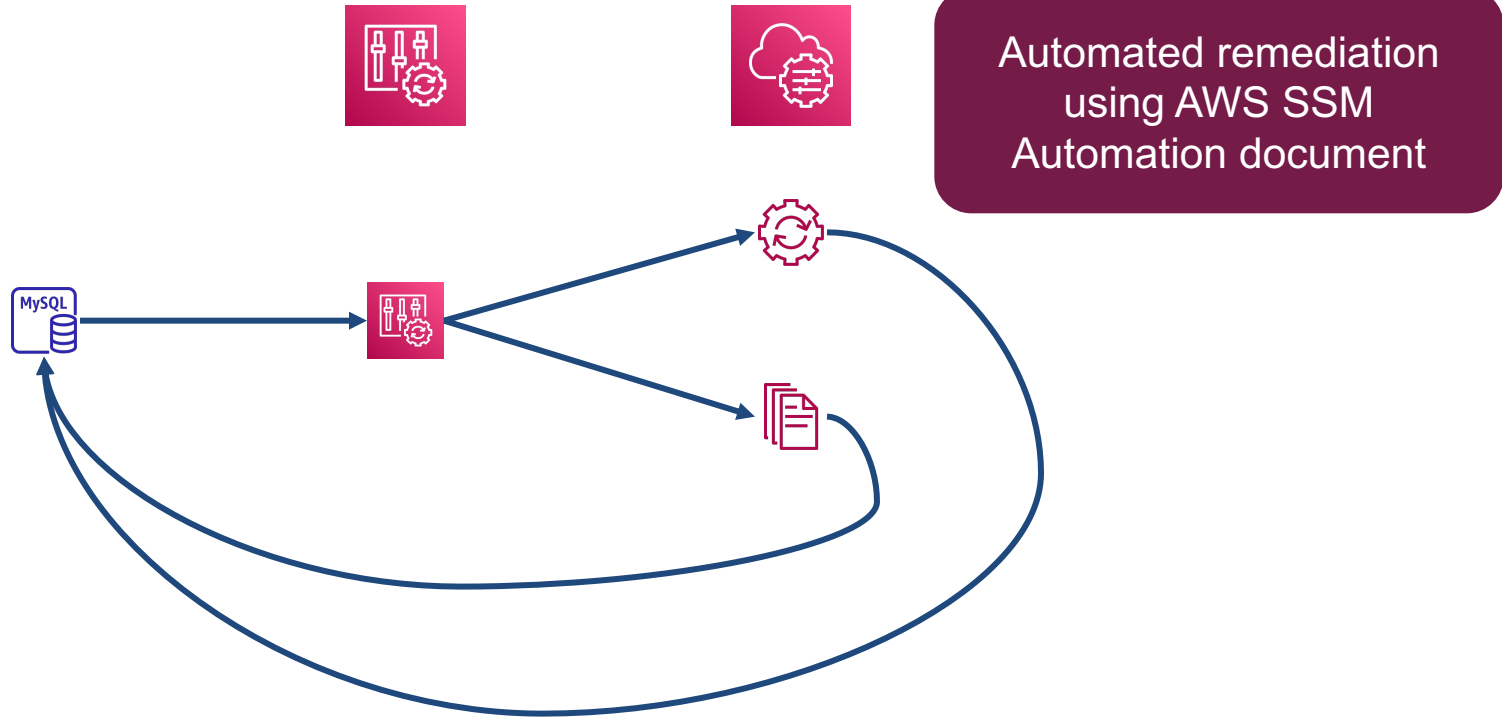
RDS instance with
Enhanced Monitoring
disabled

Config Rule Remediation Example



Manual remediation using
AWS SSM document

Config Rule Remediation Example



EventBridge Basics



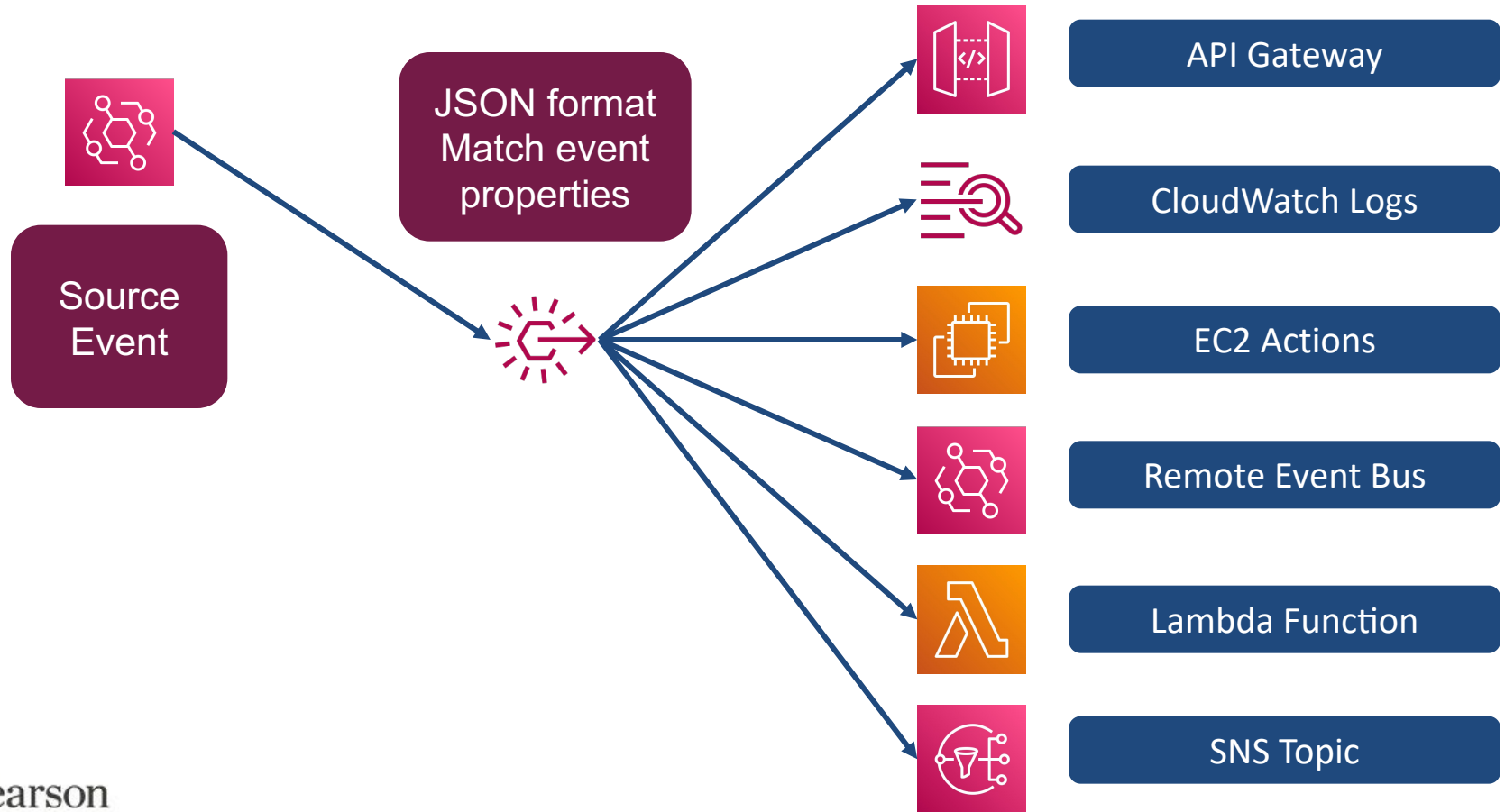
Region scope
Default Event bus
Custom Event bus
Sources and targets
Replay feature
DLQ feature

EventBridge Sources



CloudTrail API events
GuardDuty findings
Other service events
Forwarded events
Scheduled events
Custom events

EventBridge Rules



Demo

- Create event-based Config rule
- Create scheduled Config rule
- Create Config rule with active remediation
- Create EventBridge rule for GuardDuty



Creating a Global VPC Network

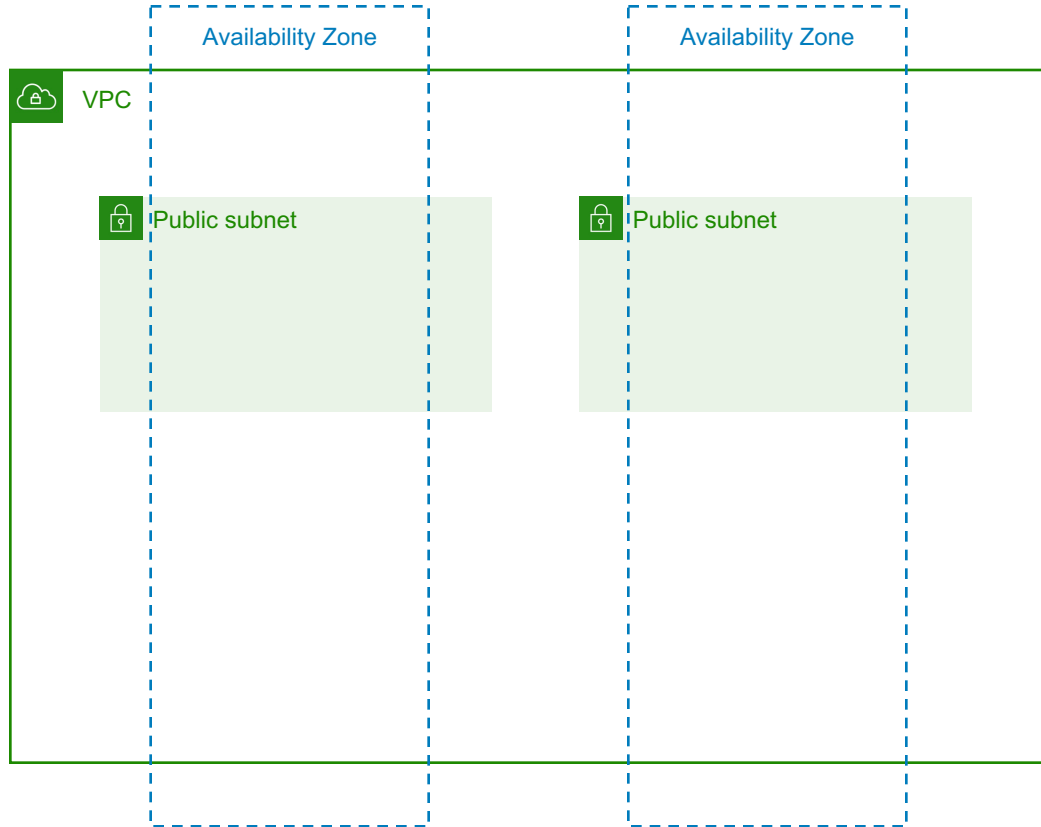
VPC Order of Operations



VPC

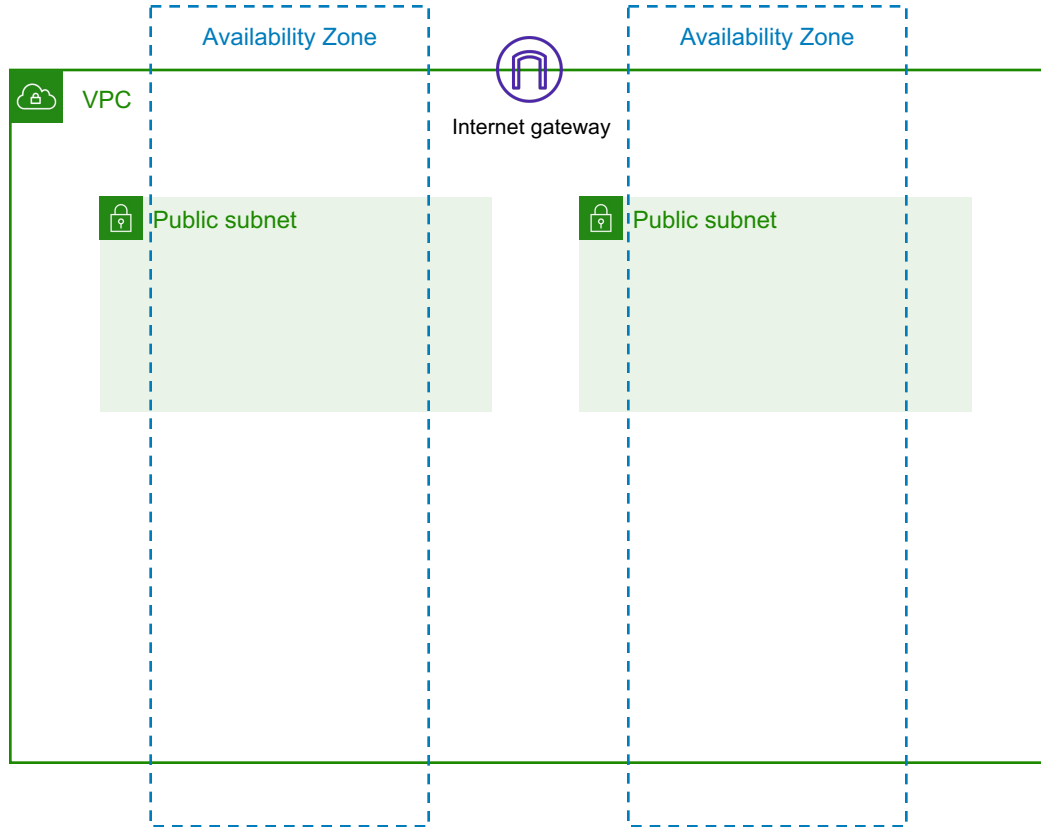
Create the VPC, including
a name and primary CIDR
range

VPC Order of Operations



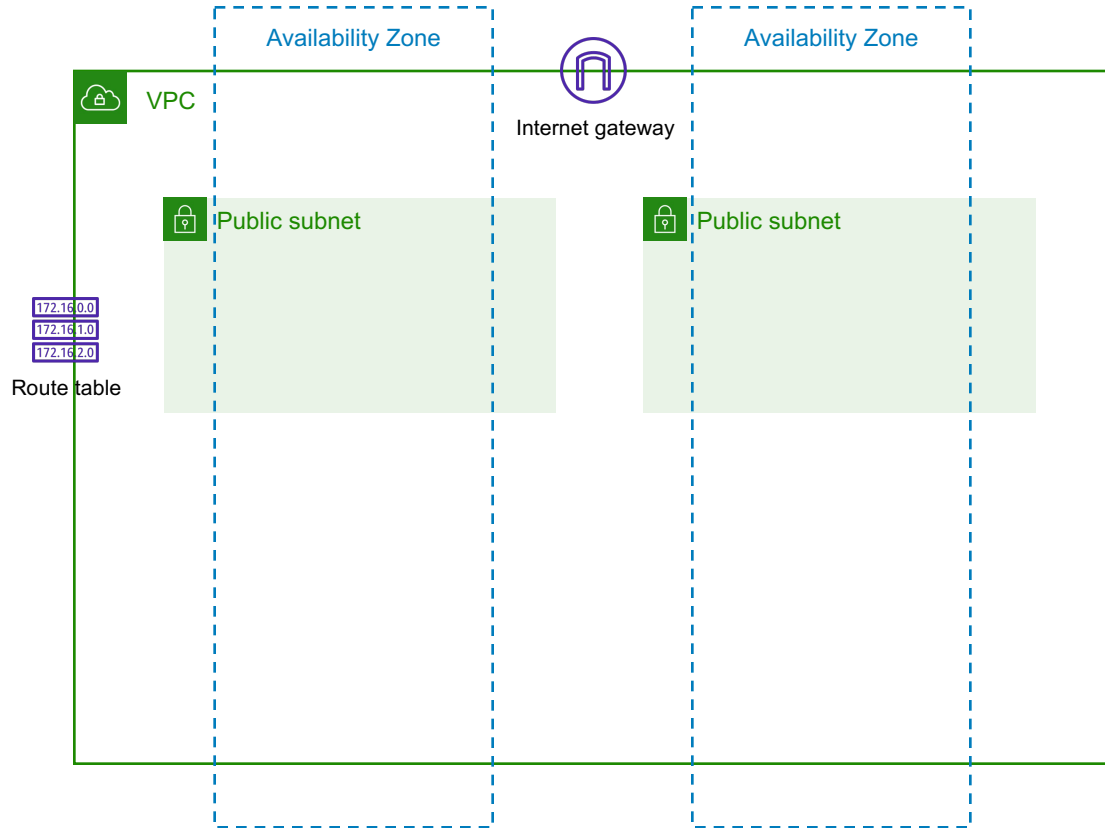
Create subnets, using AZs as required. All subnets are identical at this stage

VPC Order of Operations



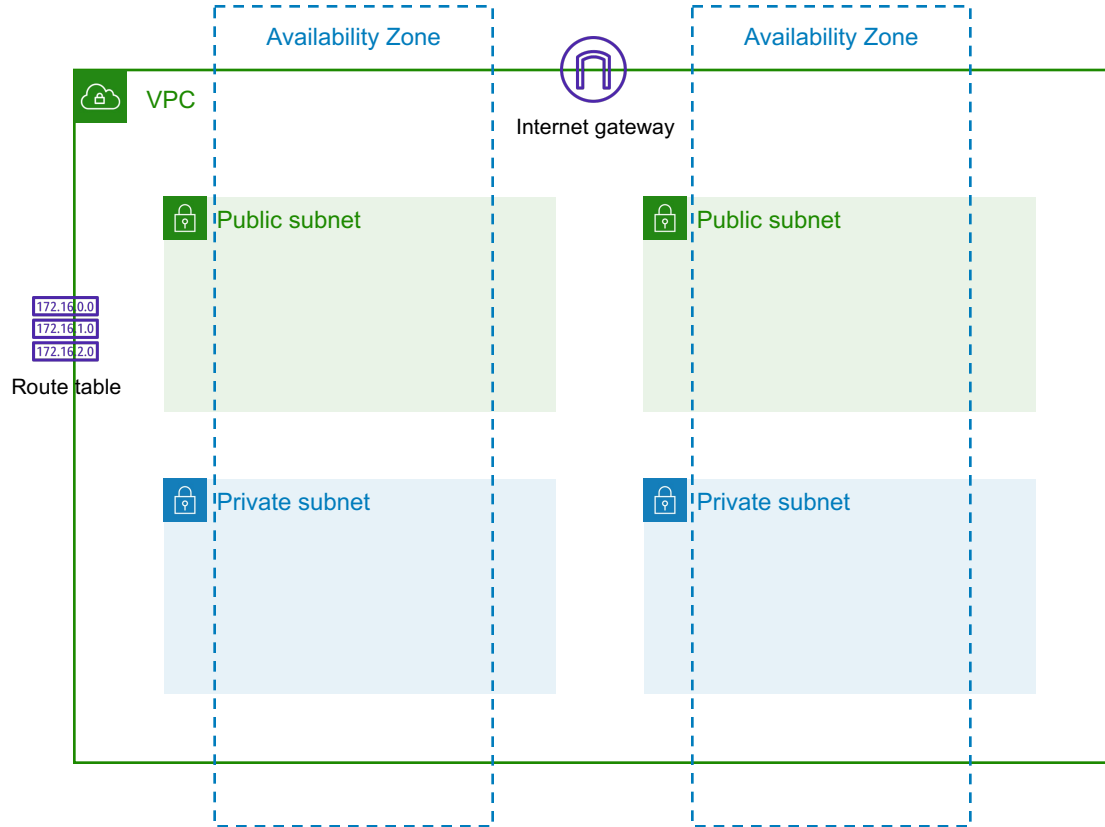
Create an IGW and attach it to the VPC (2 different actions)

VPC Order of Operations



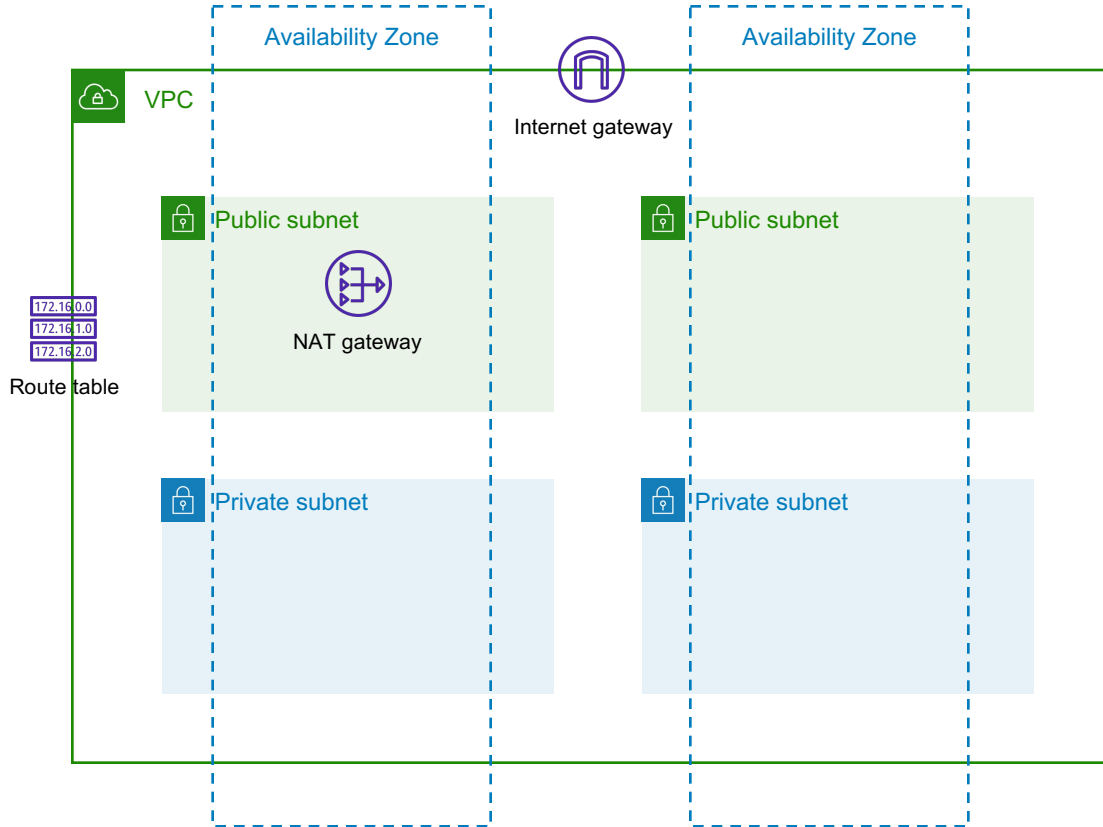
Create a route table, add a route with IGW as the target, and attach to the public subnets (3 tasks)

VPC Order of Operations



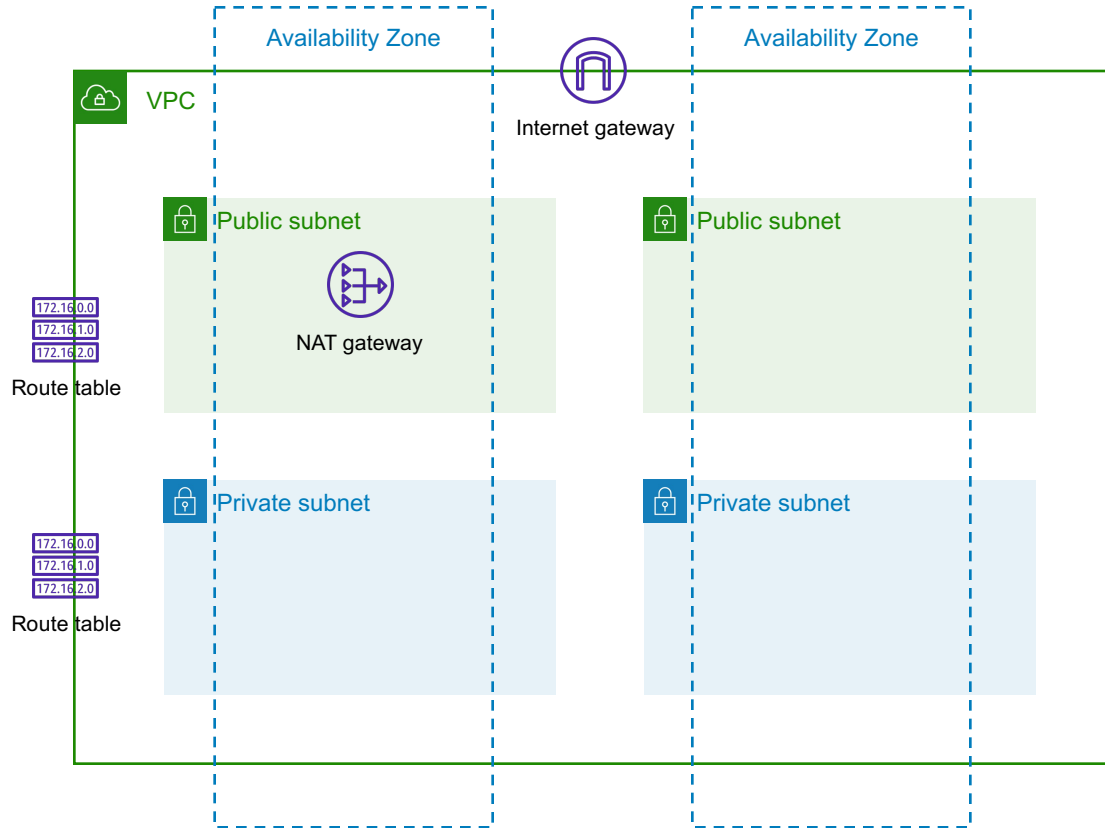
Create private subnets

VPC Order of Operations



Create a NAT Gateway
with associated EIP

VPC Order of Operations



Create a route table, add a route with NAT GW as the target, and attach to the private subnets (3 tasks)

Connectivity Options Summary



Connectivity Options Summary

	Route	SG	Policy	ENI	Subnet
GW Endpoint	✓		✓		
Interface Endpoint		✓		✓	✓

Connectivity Options Summary

	Route	SG	Policy	ENI	Subnet
GW Endpoint	✓		✓		
Interface Endpoint		✓		✓	✓
GWLB Endpoint	✓	✓		✓	✓

Connectivity Options Summary

	Route	SG	Policy	ENI	Subnet
GW Endpoint	✓		✓		
Interface Endpoint		✓		✓	✓
GWLB Endpoint	✓	✓		✓	✓
VPC Peering	✓				

Connectivity Options Summary

	Route	SG	Policy	ENI	Subnet
GW Endpoint	✓		✓		
Interface Endpoint		✓		✓	✓
GWLB Endpoint	✓	✓		✓	✓
VPC Peering	✓				
VPG	✓				

Connectivity Options Summary

	Route	SG	Policy	ENI	Subnet
GW Endpoint	✓		✓		
Interface Endpoint		✓		✓	✓
GWLB Endpoint	✓	✓		✓	✓
VPC Peering	✓				
VPG	✓				
Transit GW	✓			✓✓	✓✓

Transit GW
attachments can be
associated with
multiple AZ/subnets

Region Selection Criteria



Service availability
Co-locate with users
Co-locate with infra
Data residency
Multi-region DR

Service Selection Criteria



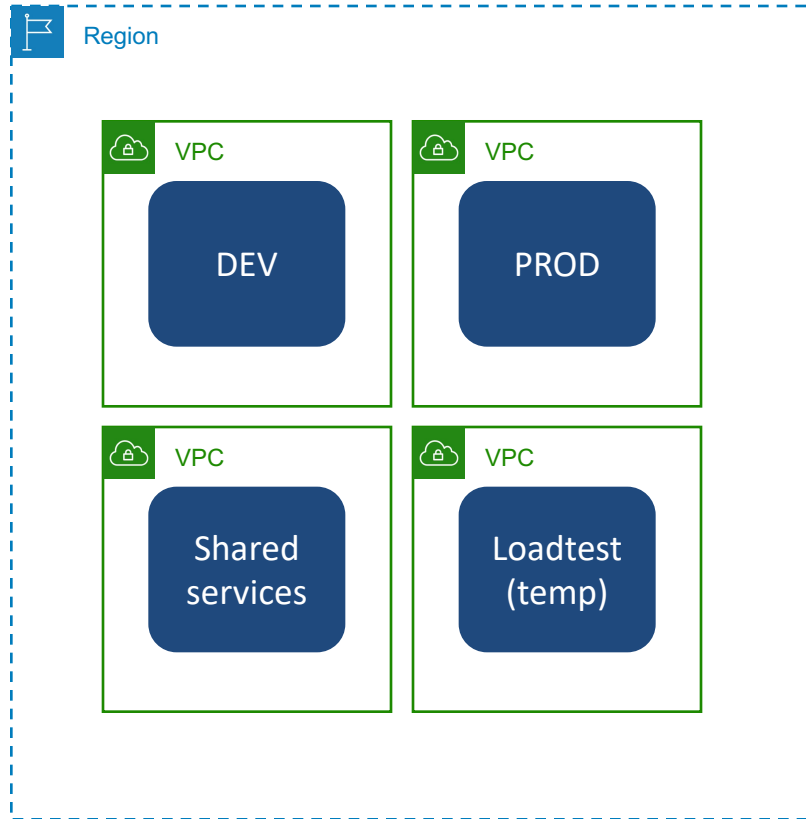
Service availability doesn't imply all features are available in the region

Check for service compliance by program (PCI, SOC, GDPR, etc.)

Service compliance doesn't imply all features are compliant

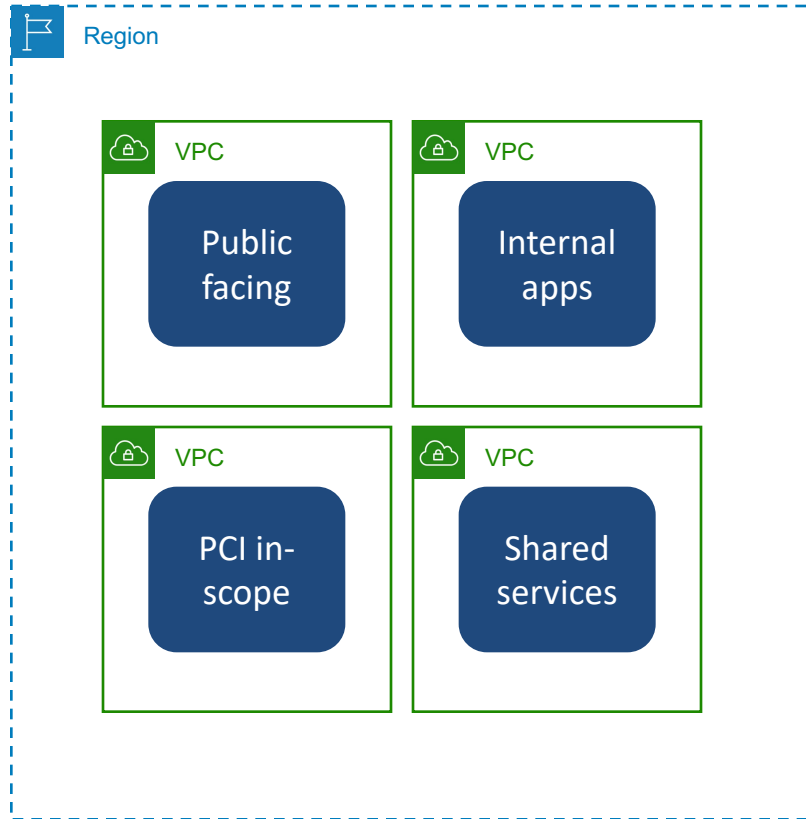
When in doubt, ask support!

VPC Workload Isolation Strategies



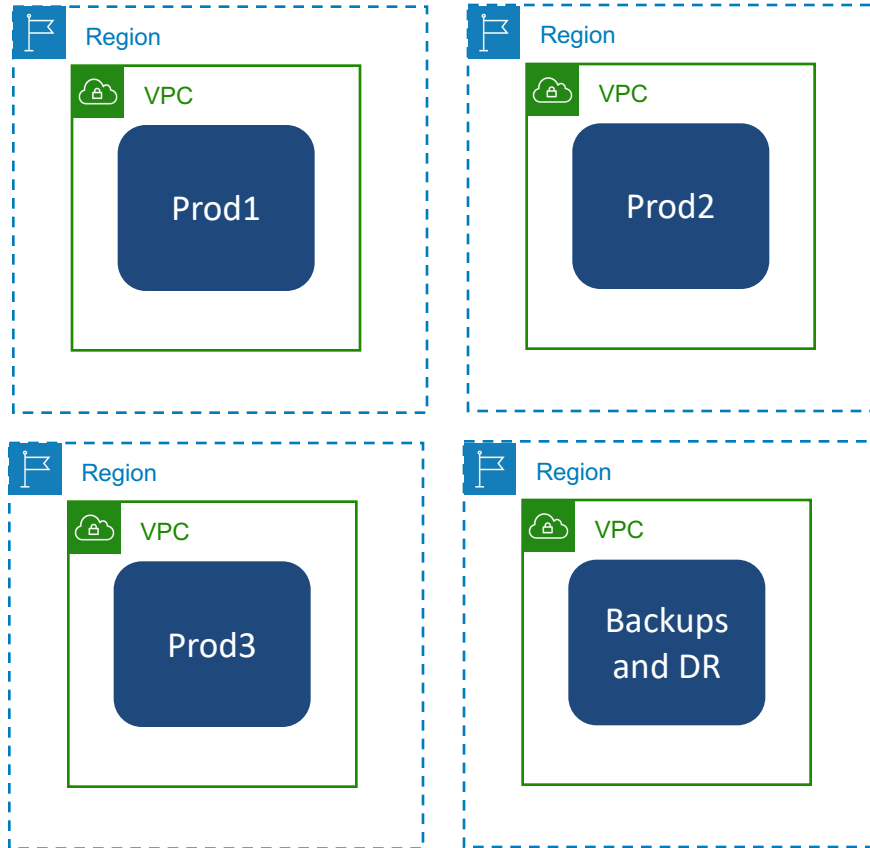
Organize by
environment

VPC Workload Isolation Strategies



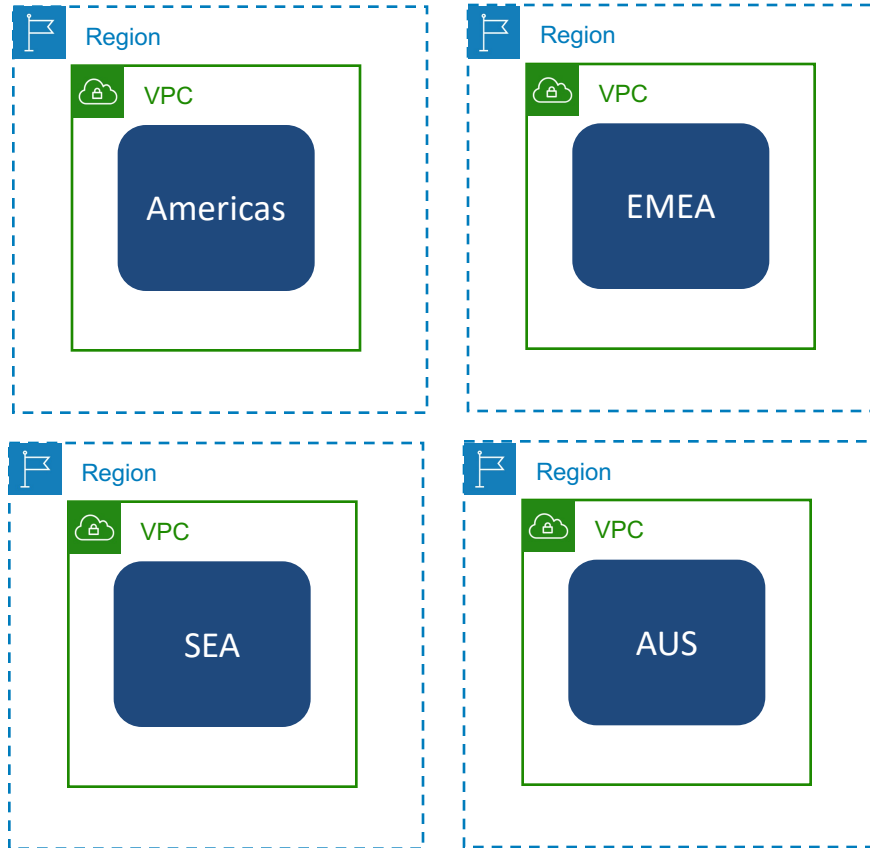
Organize by workload
compliance

VPC Workload Isolation Strategies



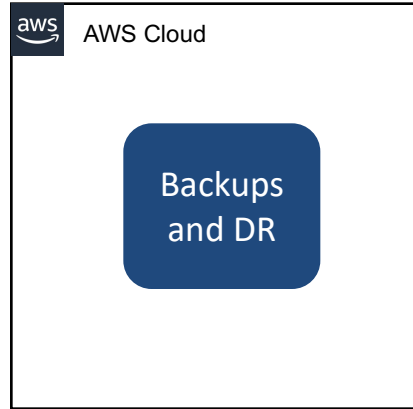
Organize by business continuity

VPC Workload Isolation Strategies

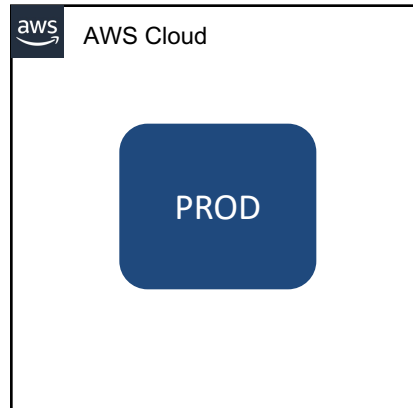
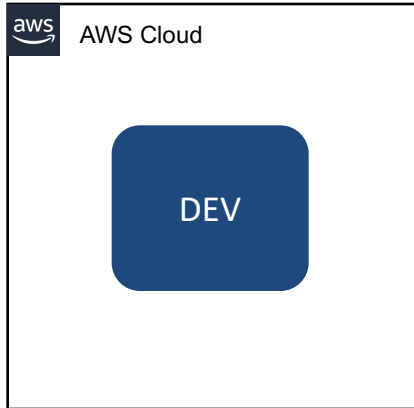


Organize by data
sovereignty

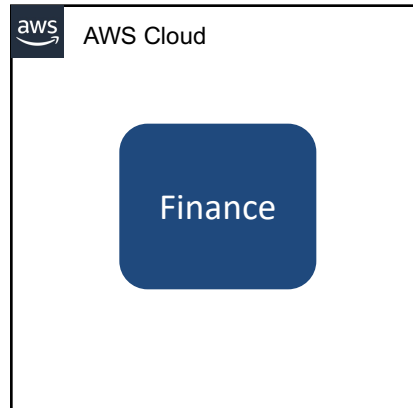
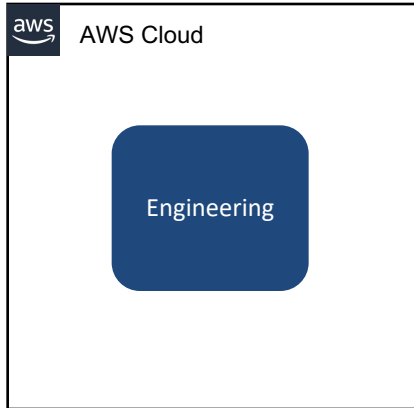
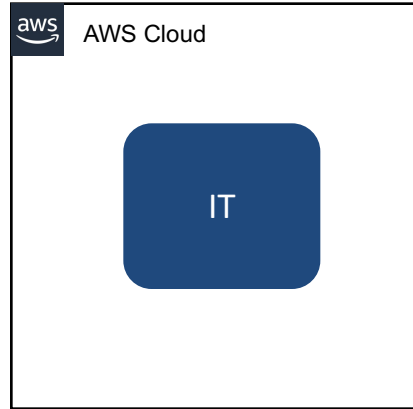
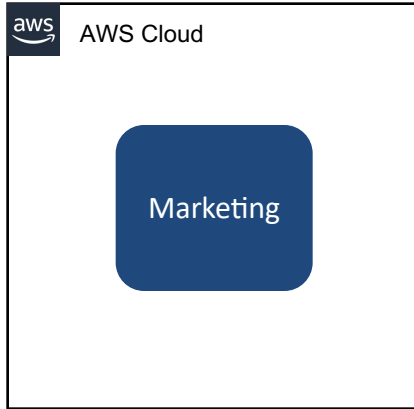
Workload Isolation Strategies



Organize by security requirements



Workload Isolation Strategies



Organize to match
company hierarchy

Demo

Deploy VPCs in different regions (Terraform)

Connect VPCs using peering connections

Connect VPCs using Transit GW



Deploying EC2

EC2 Launch Options - Console

What are the tradeoffs when launching an EC2 instance using the AWS Console?

Path of least
resistance
Always current
Semi-helpful
suggestions
Semi-helpful error
codes

Can't automate
Can't scale
Human error
Frequent UI
changes

EC2 Launch Options - CLI

Ever tried embedding JSON syntax inside CLI syntax? Easy to make mistakes!

This command line gets ridiculous, very quickly.
Is there a better way?

```
run_instances
[--block-device-mappings <value>]
[--image-id <value>]
[--instance-type <value>]
[--ipv6-address-count <value>]
[--ipv6-addresses <value>]
[--kernel-id <value>]
[--key-name <value>]
[--monitoring <value>]
[--placement <value>]
[--ramdisk-id <value>]
[--security-group-ids <value>]
[--security-groups <value>]
[--subnet-id <value>]
[--user-data <value>]
[--additional-info <value>]
[--client-token <value>]
[--disable-api-termination | --enable-api-termination]
[--dry-run | --no-dry-run]
[--ebs-optimized | --no-ebs-optimized]
[--iam-instance-profile <value>]
[--instance-initiated-shutdown-behavior <value>]
[--network-interfaces <value>]
[--private-ip-address <value>]
[--elastic-gpu-specification <value>]
[--elastic-inference-accelerators <value>]
[--tag-specifications <value>]
[--launch-template <value>]
[--instance-market-options <value>]
[--credit-specification <value>]
[--cpu-options <value>]
[--capacity-reservation-specification <value>]
[--hibernation-options <value>]
[--license-specifications <value>]
[--count <value>]
[--secondary-private-ip-addresses <value>]
[--secondary-private-ip-address-count <value>]
[--associate-public-ip-address | --no-associate-public-ip-address]
[--cli-input-json <value>]
[--generate-cli-skeleton <value>]
```

What about embedding bash/powershell syntax inside CLI syntax?
Good luck with that!

Look at these, tucked all the way at the end of the option list!

EC2 Launch Options - CLI

```
aws ec2 run-instances --generate-cli-skeleton
```

redirect output to text file

edit text file as per launch requirements

check the file into your source code repo

```
aws ec2 run-instances --cli-input-json <text file> --dry-run
```

```
aws ec2 run-instances --cli-input-json <text file>
```

EC2 Image Builder - Concepts



AMI



Components



Image Pipeline

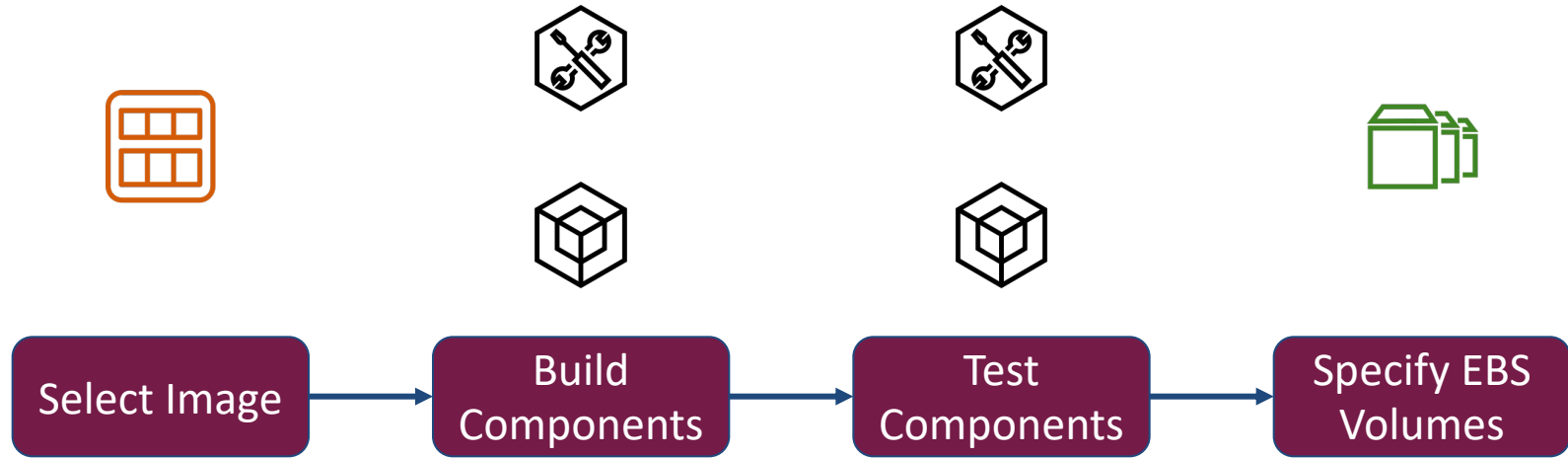
Config Phases

Image Recipe

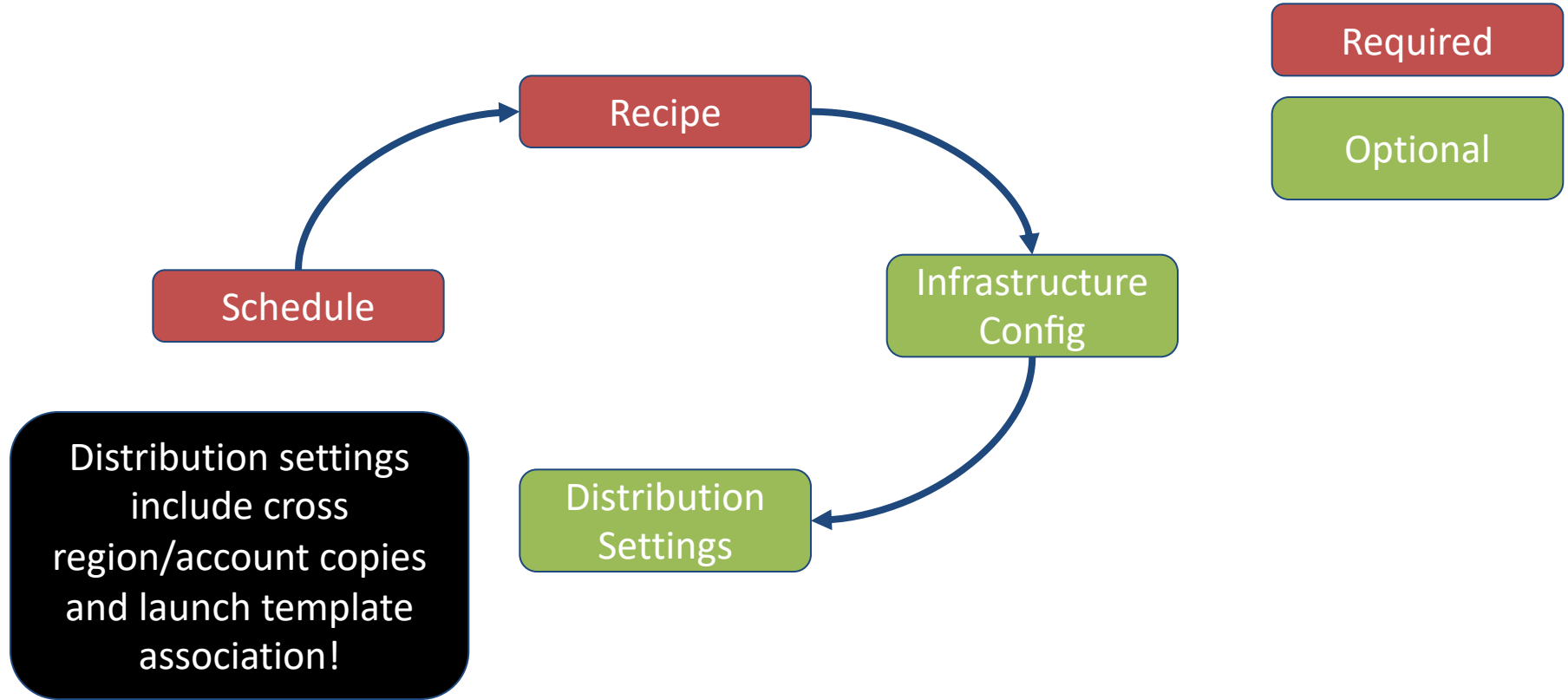
Infrastructure
Config

Distribution
Settings

EC2 Image Builder - Recipe



EC2 Image Builder - Pipeline

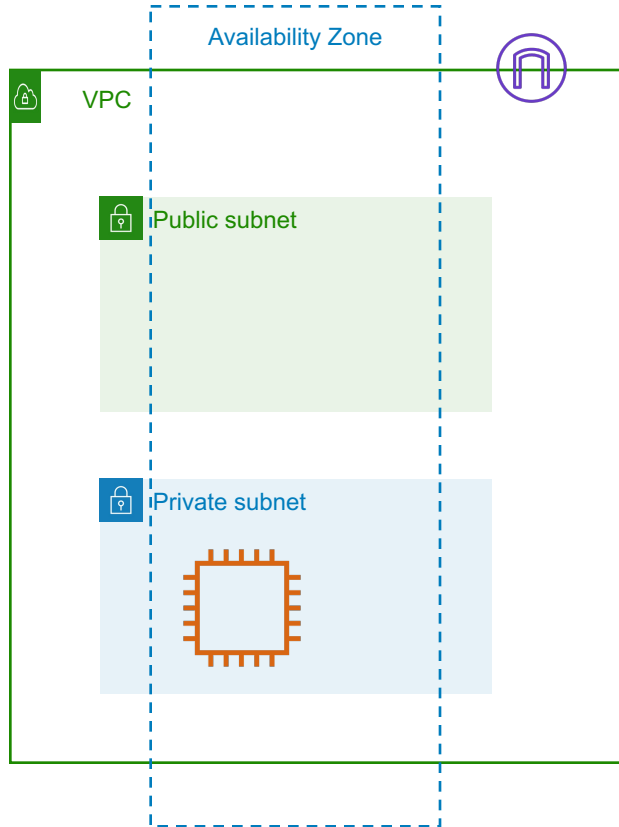


Create AMI using EC2 Image Builder



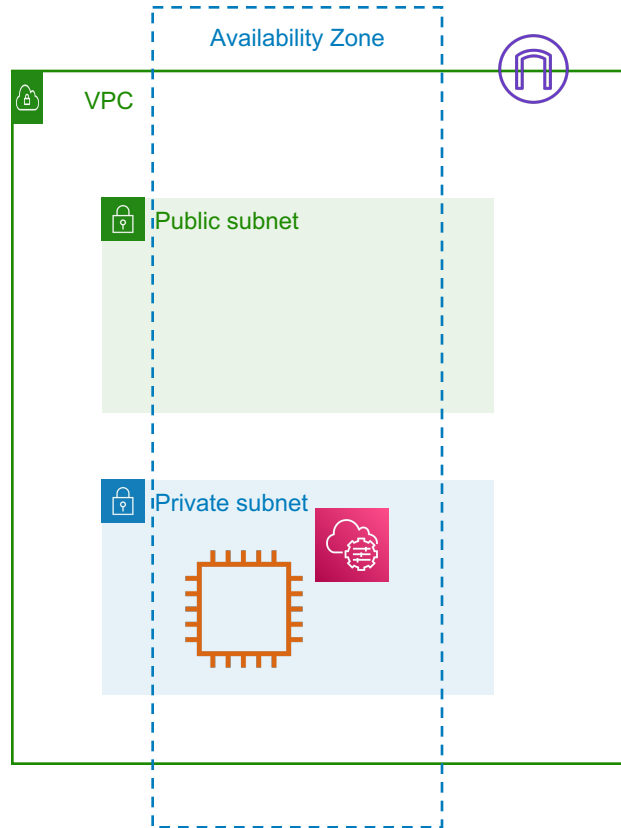
EC2 OS Operations

SSM Patch Manager Prerequisites



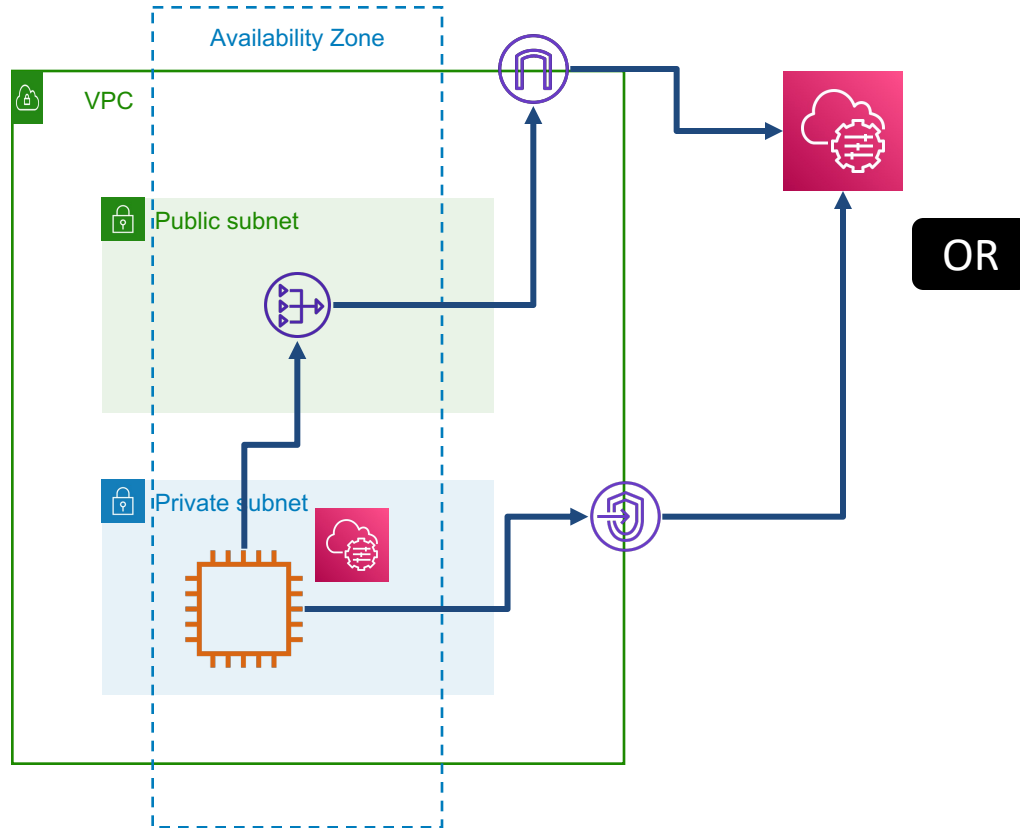
The instance must be running a supported OS

SSM Patch Manager Prerequisites



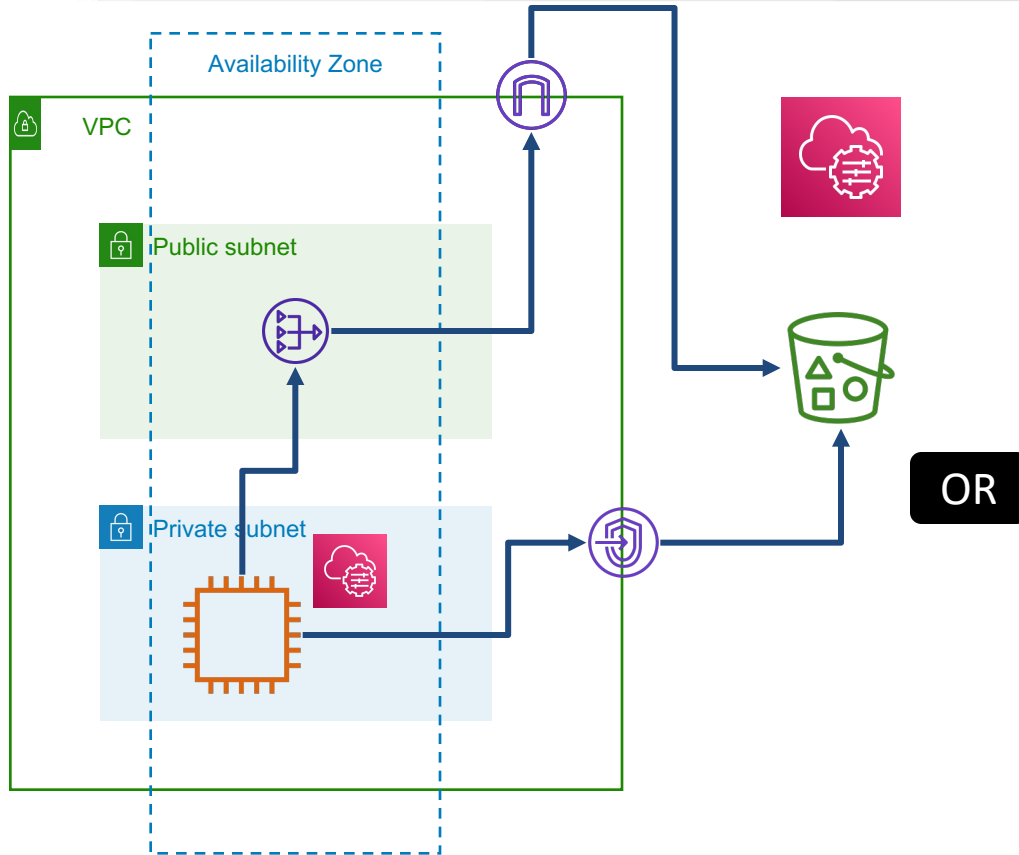
The instance must have the SSM Agent installed

SSM Patch Manager Prerequisites



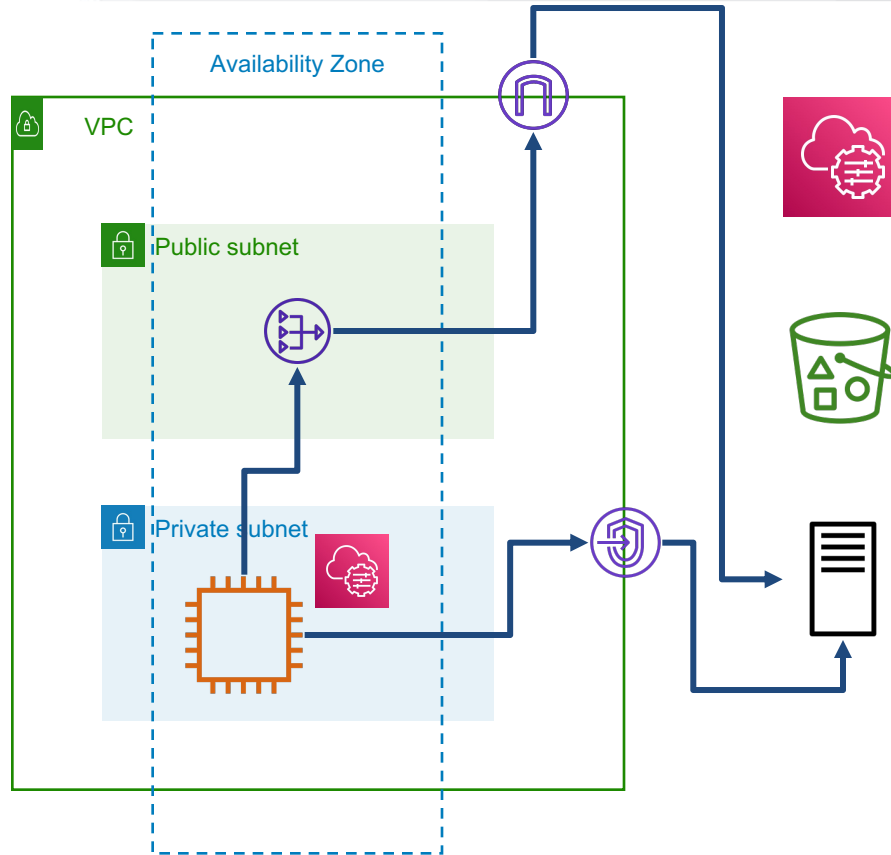
The SSM Agent must be able to access the Systems Manager service API endpoint

SSM Patch Manager Prerequisites



The SSM Agent must be able to access the SSM managed S3 buckets

SSM Patch Manager Prerequisites



The SSM Agent must be able to access the patch source repos (unique per OS type)

SSM Patch Manager Flow

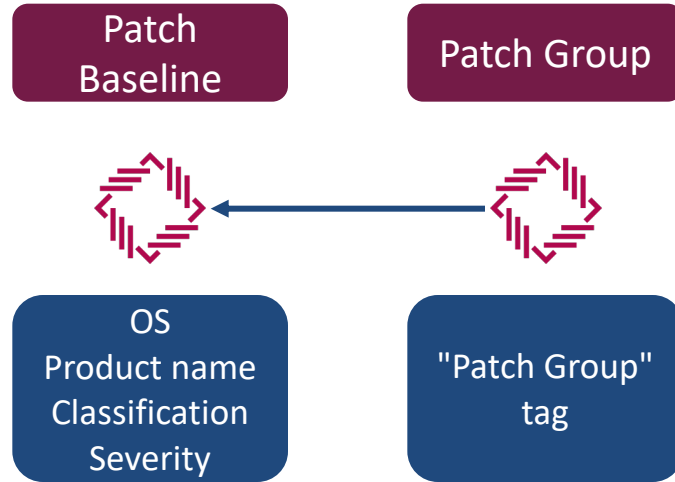
Patch
Baseline



OS
Product name
Classification
Severity

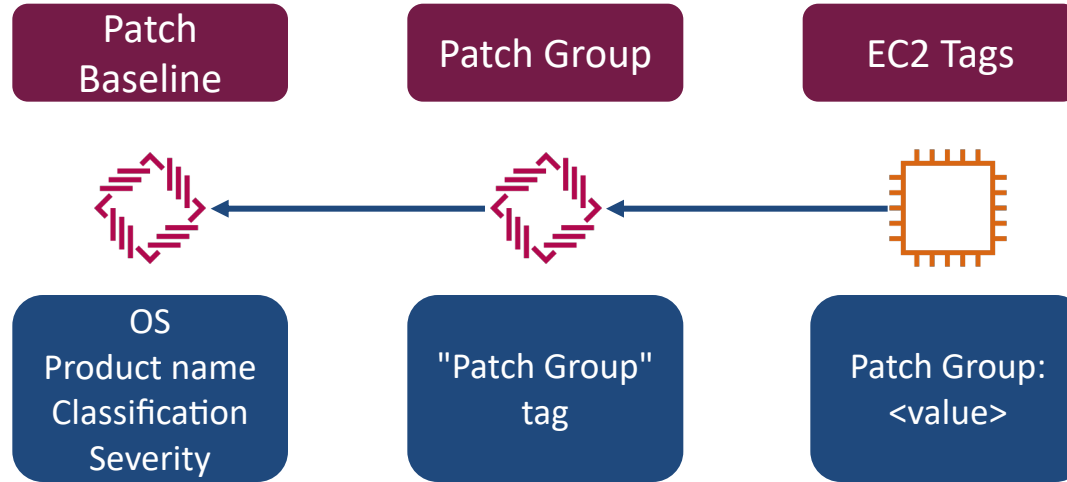
There are both
managed and custom
patch baselines,
including defaults for
each OS

SSM Patch Manager Flow



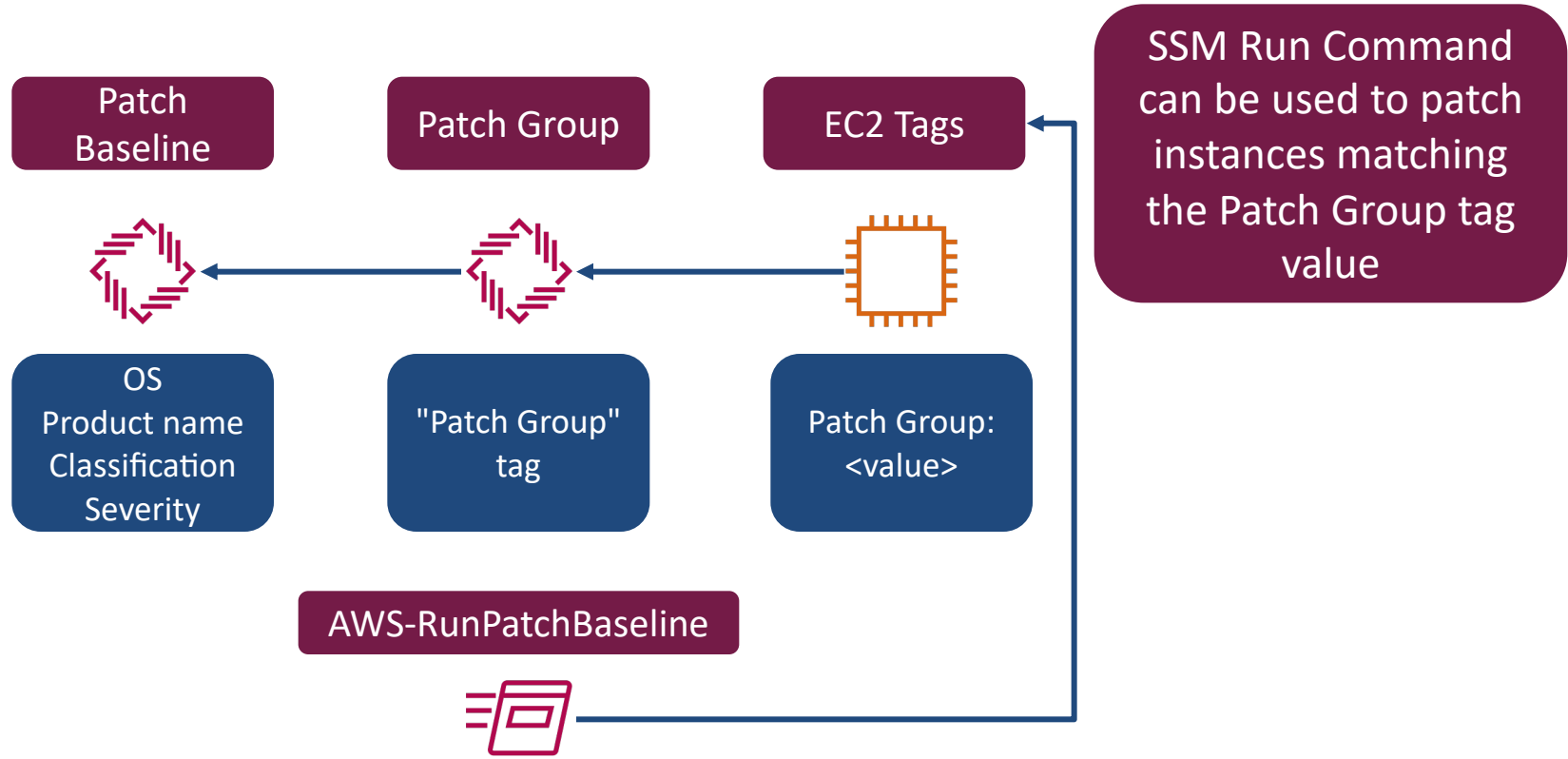
Patch Groups are associated with Patch Baselines

SSM Patch Manager Flow



The instance requires a Patch Group tag with a value that matches the SSM Patch Group

SSM Patch Manager Flow

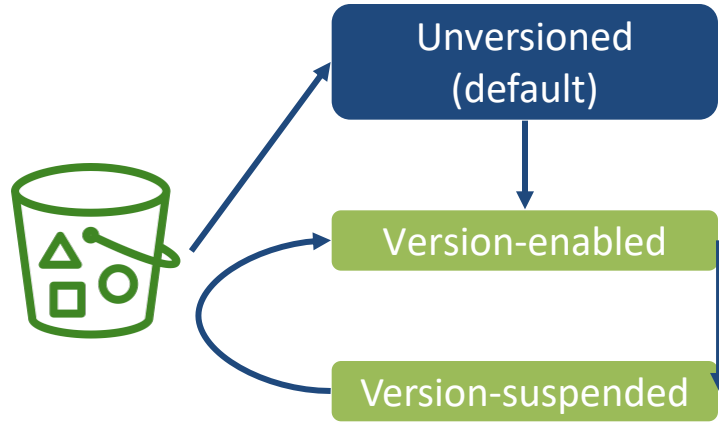


Implement SSM Patch Manager
Explore operations using Run Command



Creating and Maintaining S3 Buckets

S3 Versioning



Versioning is a good way to avoid accidental deletion

Version ID attached to each version of an object

Delete operation attaches a delete marker to the object

S3 Versioning - Considerations

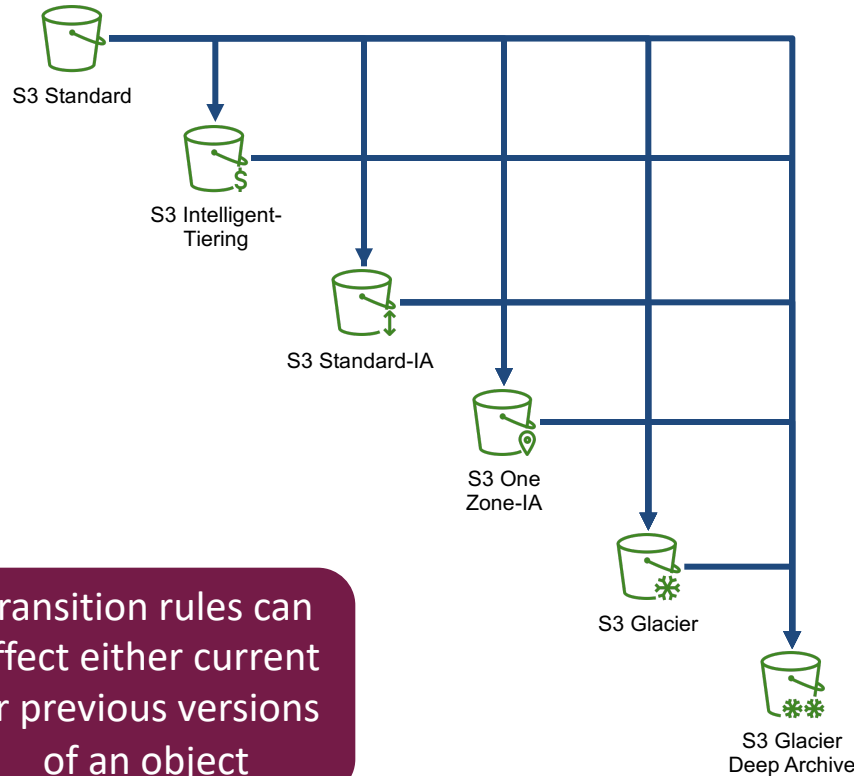


Cost of many versions

Performance of many versions

More complex lifecycle rules

Lifecycle Rules - Transition & Expire



Objects can be expired from any storage class and version

Transition rules can affect either current or previous versions of an object

S3 Lifecycle Rules - Options



Transition current versions

Transition previous
versions

Expire current versions

Delete expired delete
markers

Delete incomplete
multipart uploads

S3 Lifecycle Rules - Considerations



Object size

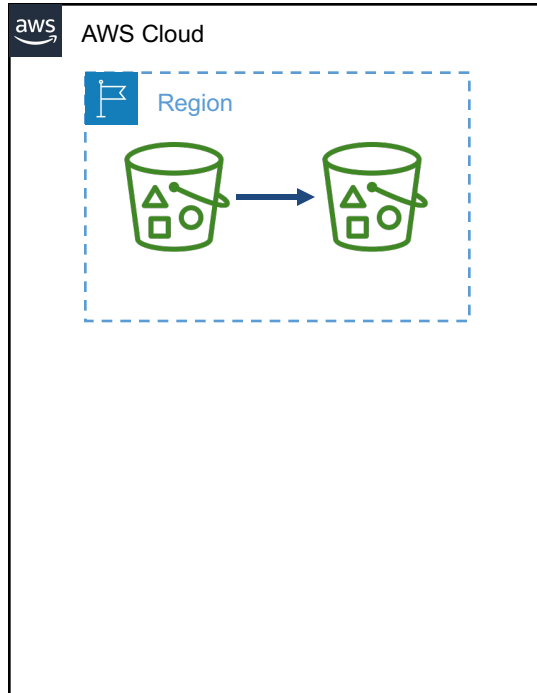
Object age requirements

Bucket or prefix scope

Tag scope

Conflicting rules

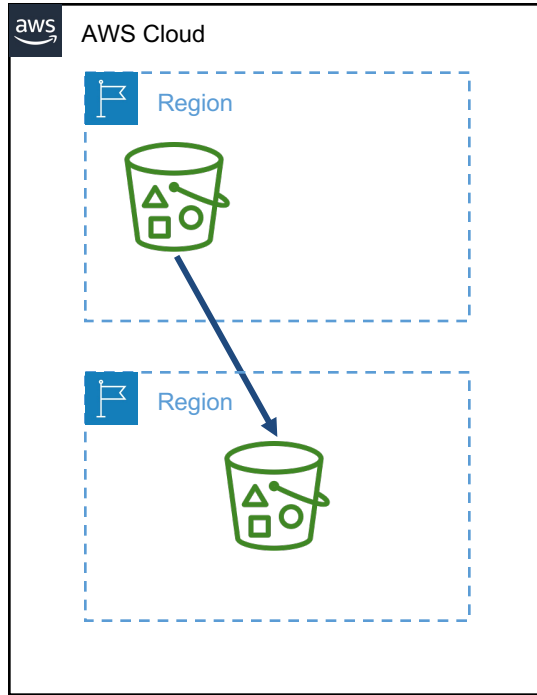
Replication Options



Same-region, same-account replication

All replication requires versioning enabled at source and destination

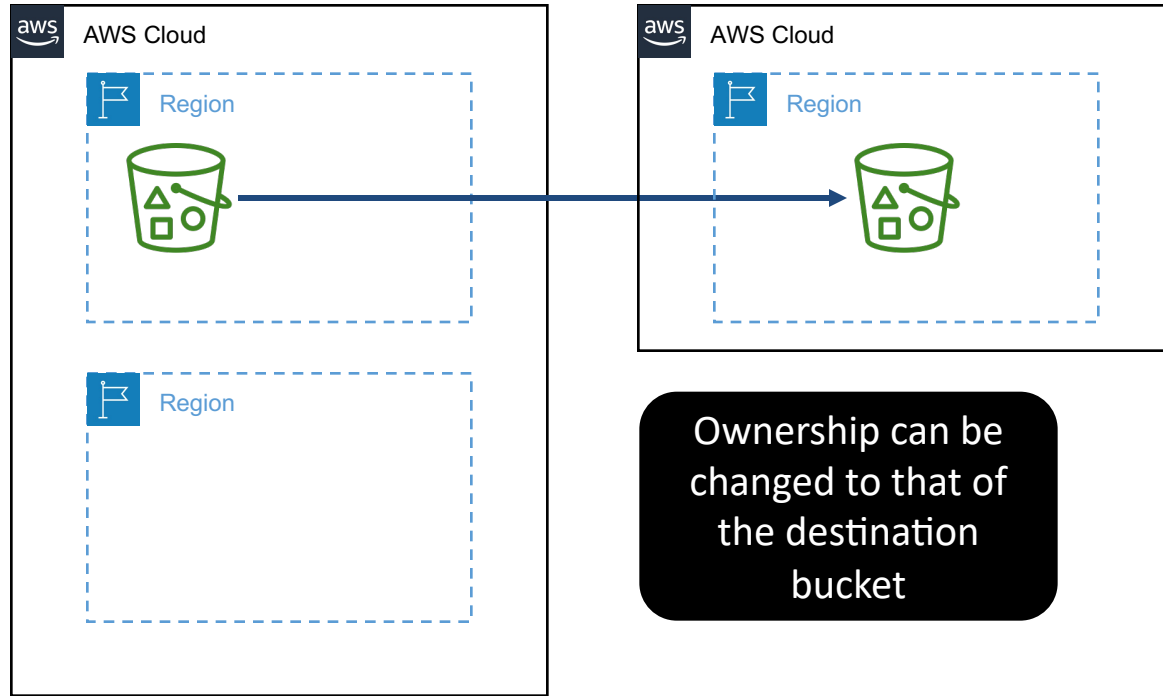
Replication Options



Cross-region, same-account replication

All replication
requires an IAM
Role for permissions

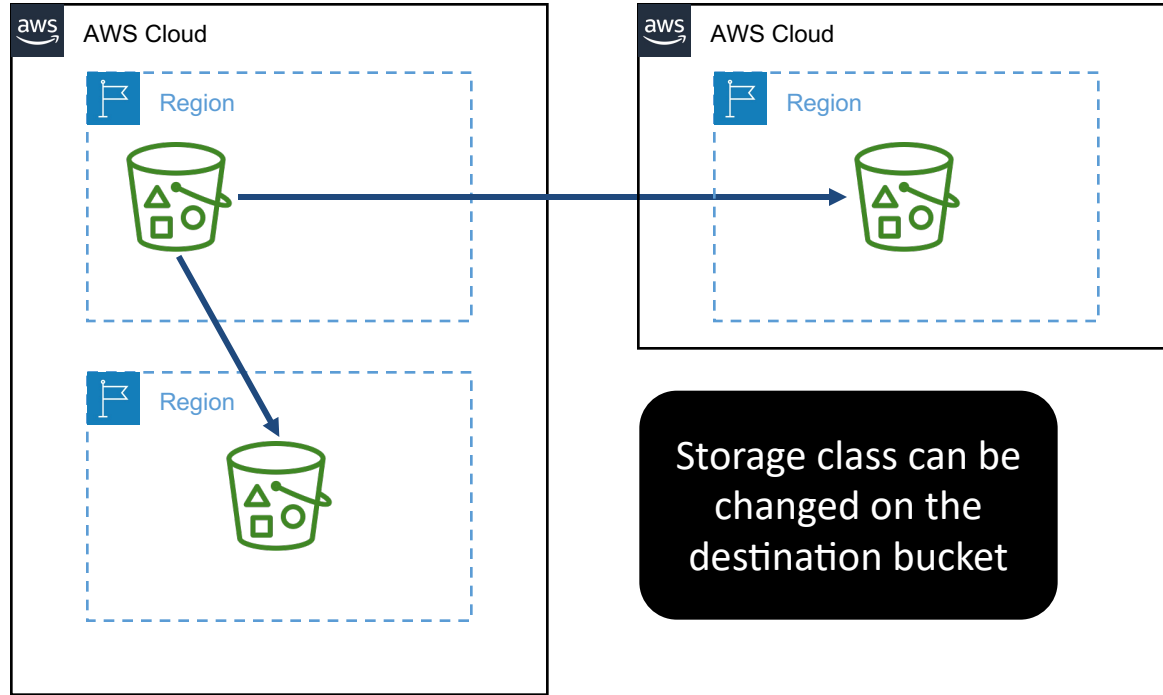
Replication Options



Cross-region, cross-account replication

Ownership can be changed to that of the destination bucket

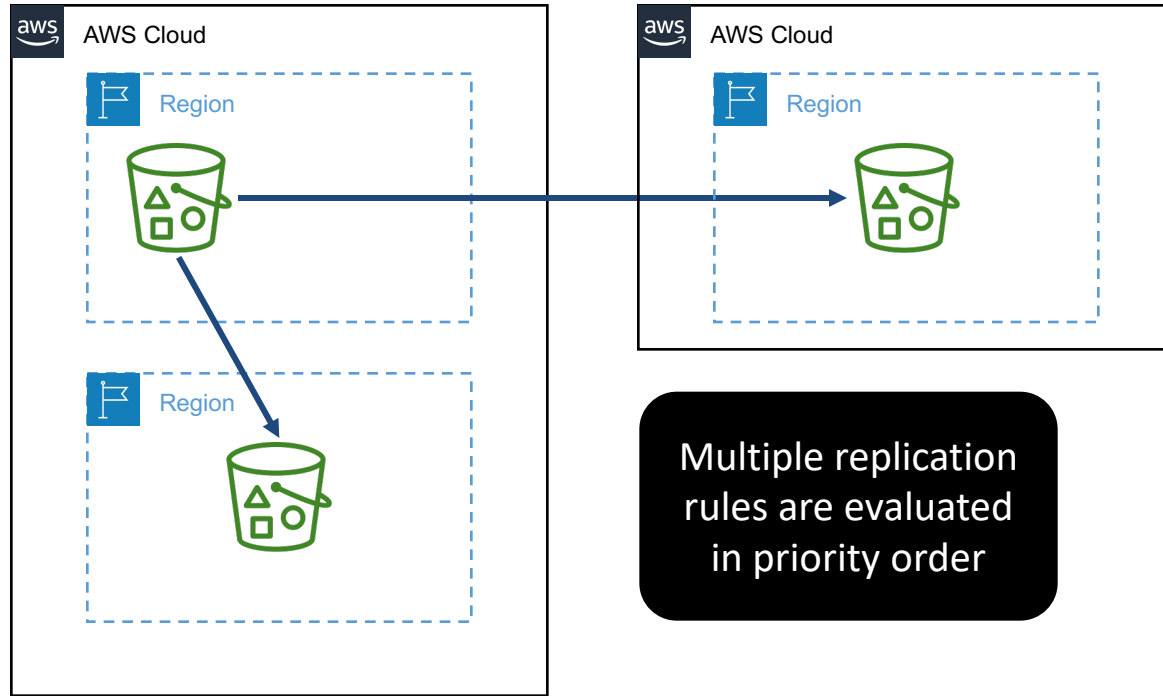
Replication Options



Replication to
multiple bucket
destinations

Storage class can be
changed on the
destination bucket

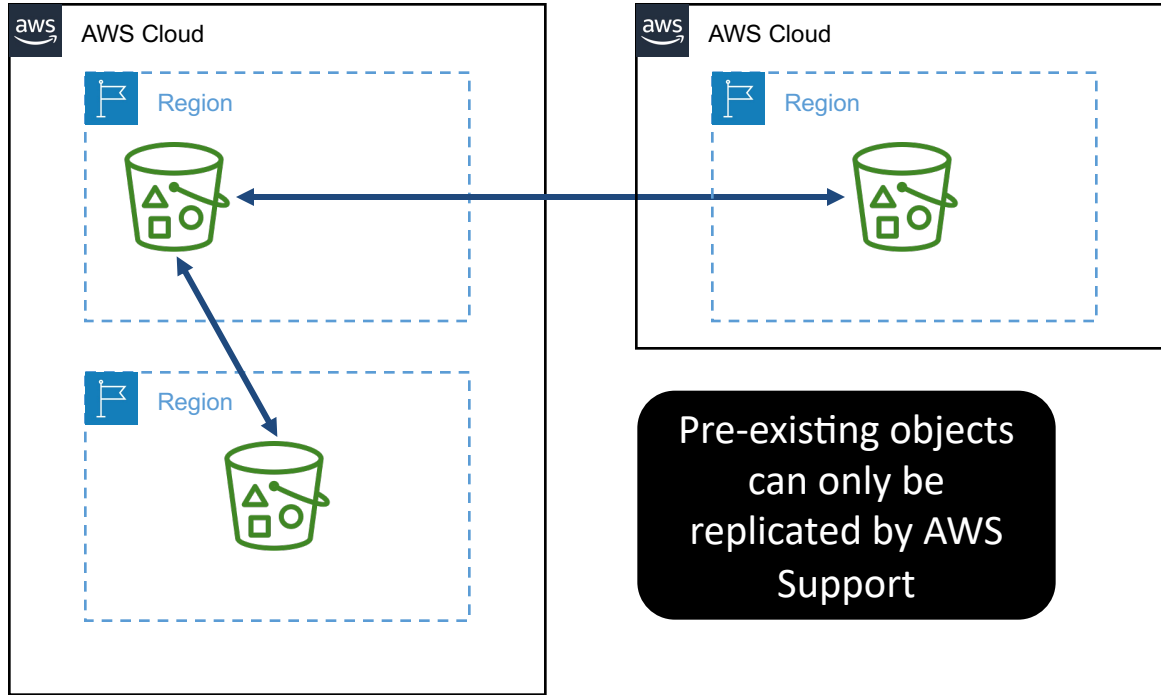
Replication Options



Replication to
multiple bucket
destinations

Multiple replication
rules are evaluated
in priority order

Replication Options



Multi-way
replication between
2+ buckets

Pre-existing objects
can only be
replicated by AWS
Support

DEMO

Use CLI to create S3 bucket with full configuration

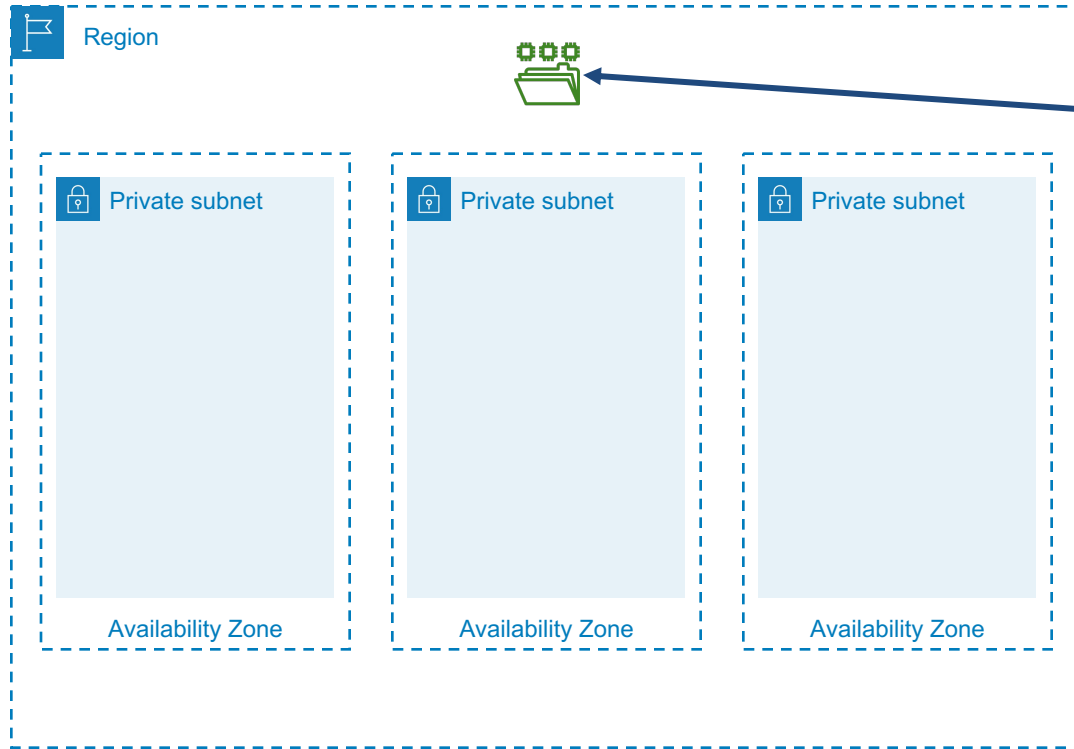
Explore monitoring options

Explore S3 Batch options



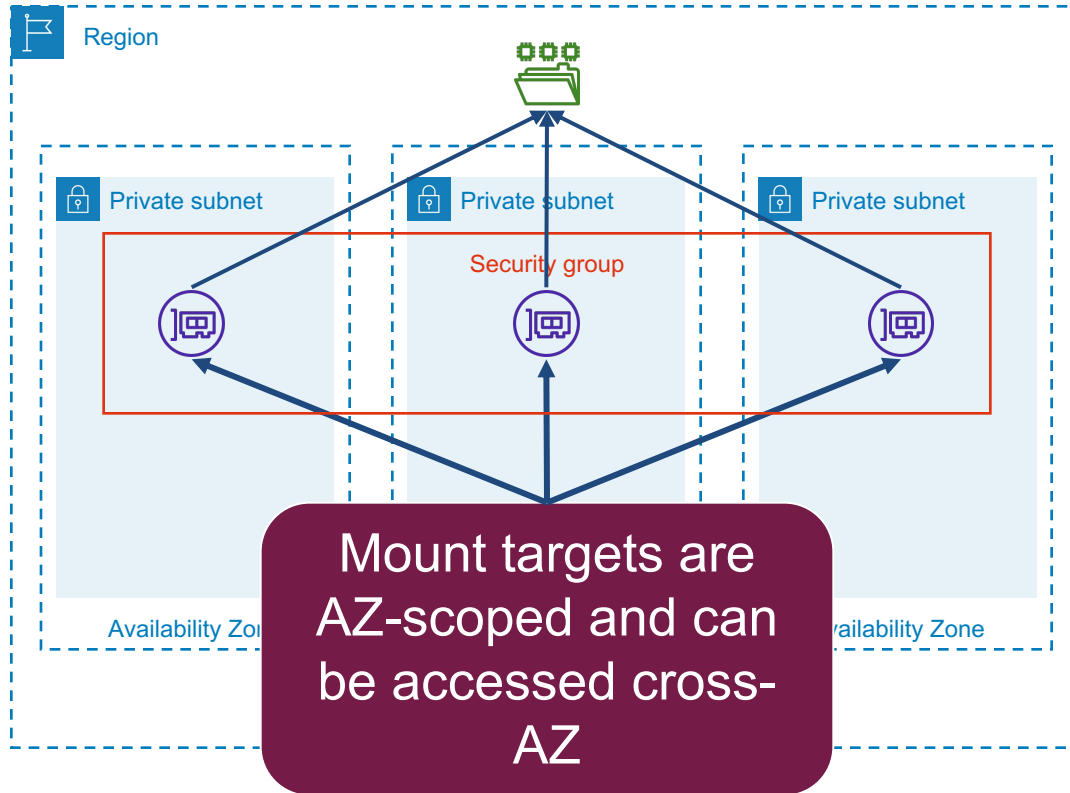
Deploying EFS

Elastic Filesystem (EFS)



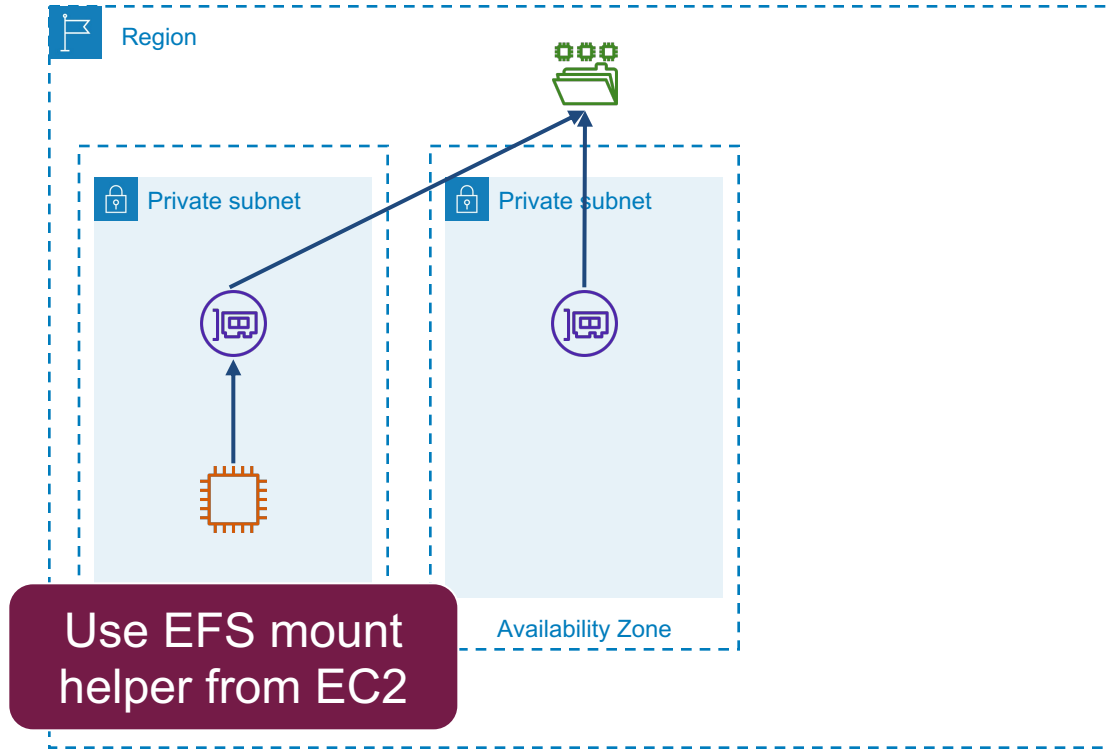
EFS Filesystem
object is region-
scoped and durable

Elastic Filesystem (EFS)

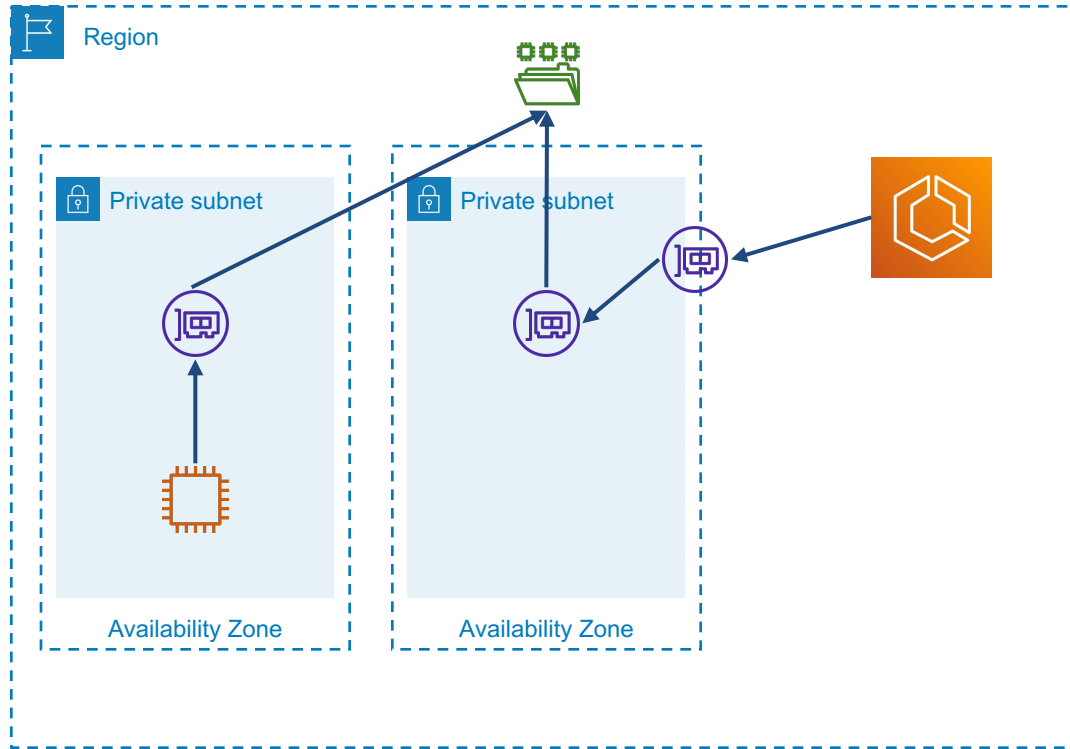


Mount targets can specify directory and userid

Elastic Filesystem (EFS) Mounts

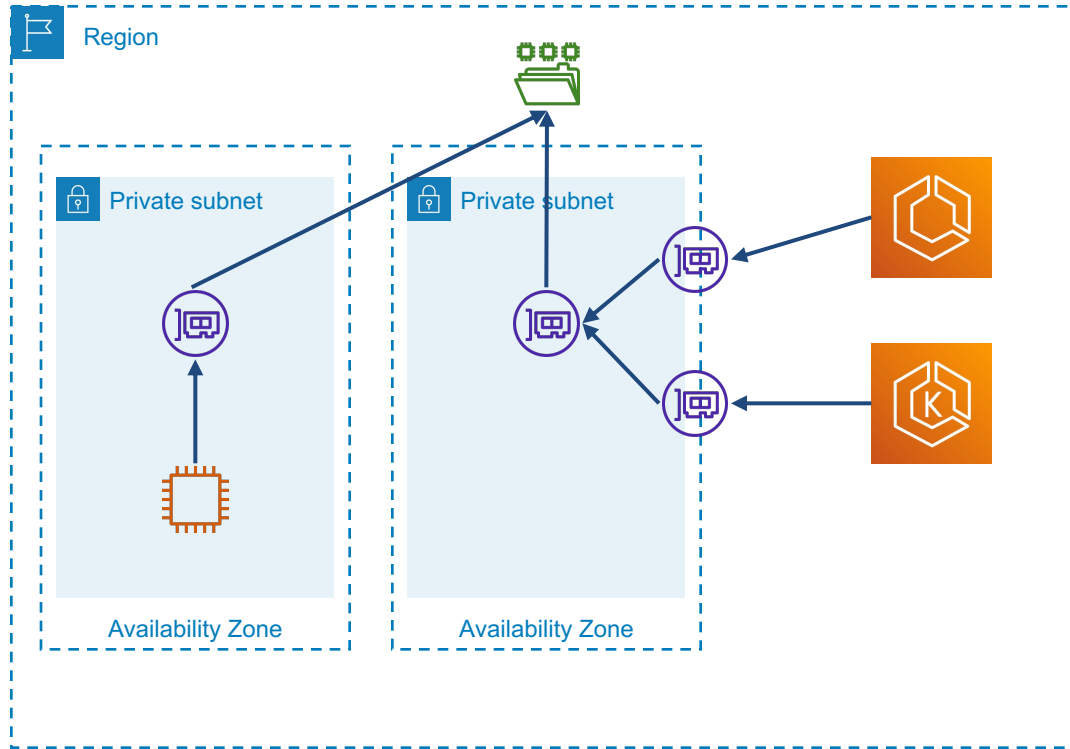


Elastic Filesystem (EFS) Mounts



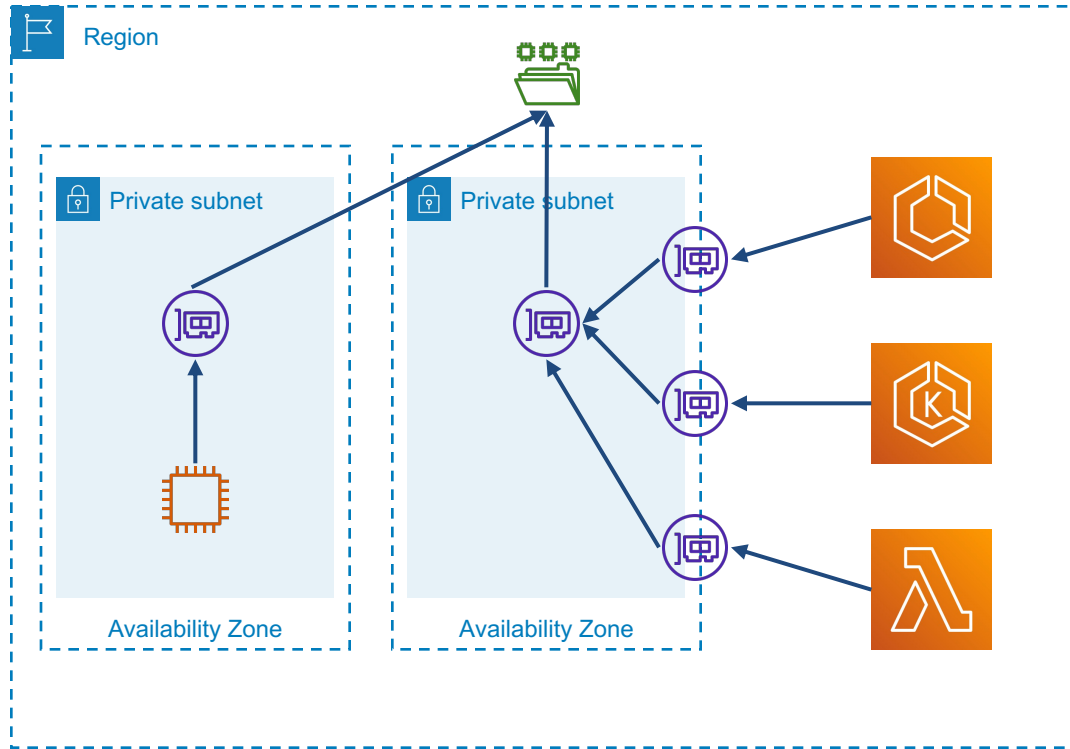
Mount on ECS
containers

Elastic Filesystem (EFS) Mounts



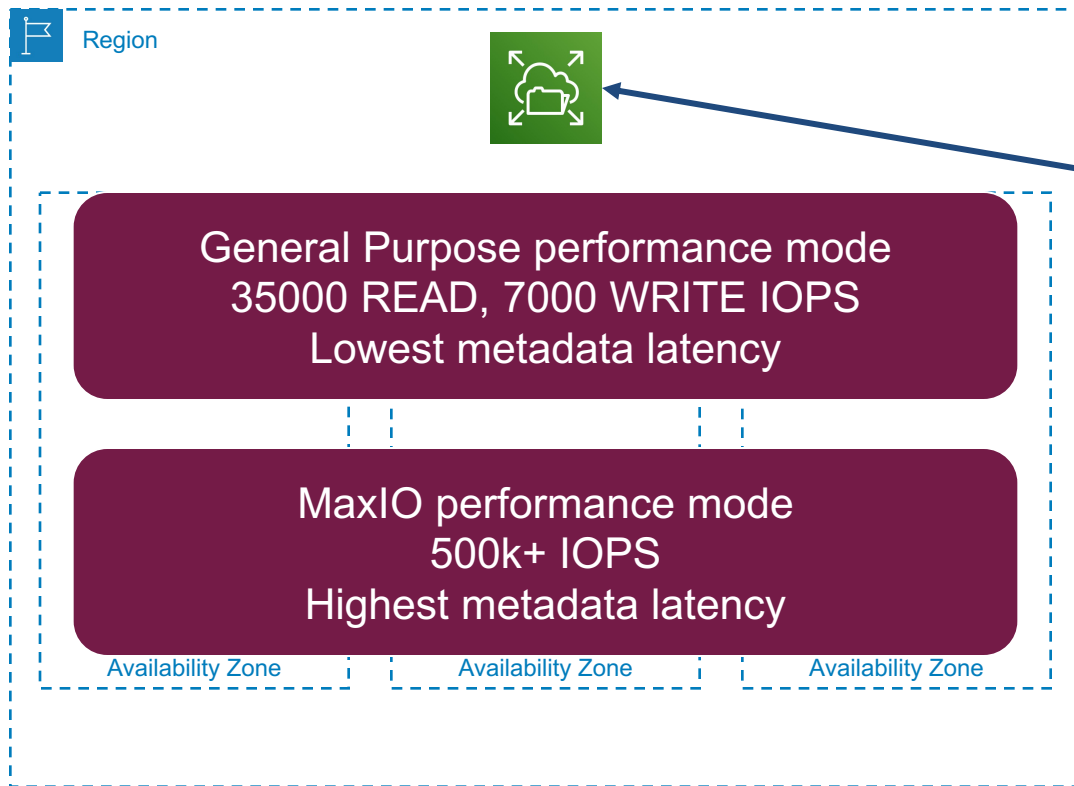
Mount on EKS
containers

Elastic Filesystem (EFS) Mounts



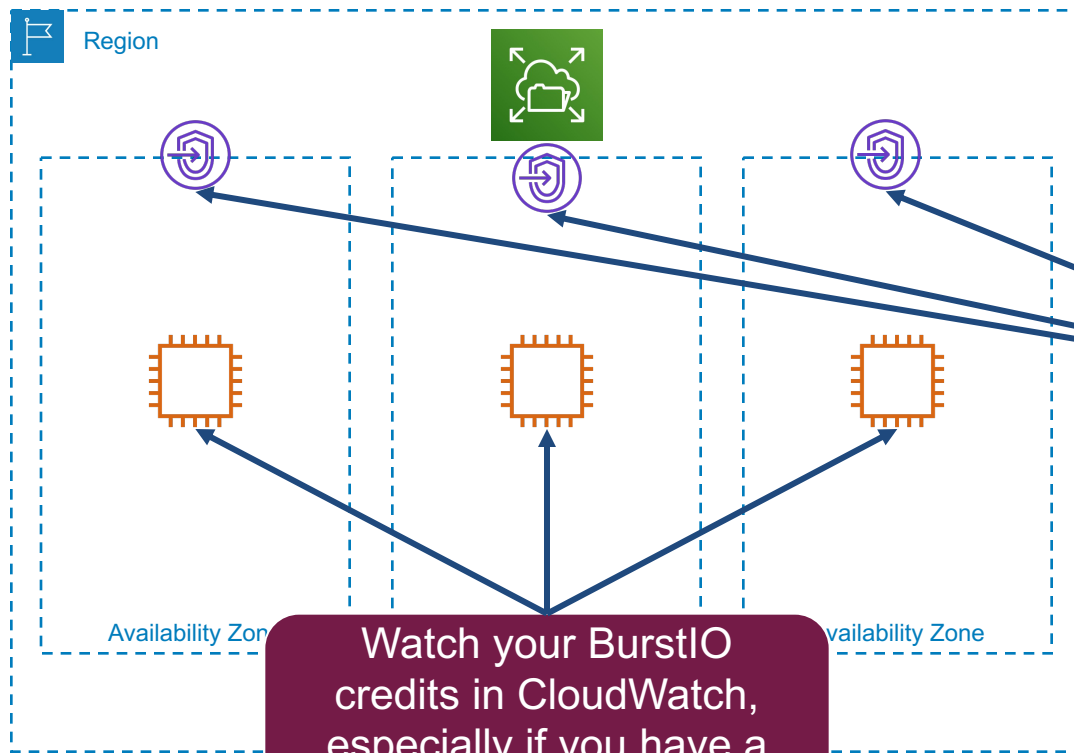
Mount on Lambda
functions

EFS Performance



EFS File system resource
10GB/s+ throughput
Depends on region
500MB/s per client
Latency: unpublished but
can be 1ms

EFS Performance



Make sure you use the mount point in the SAME AZ as your client node!

Watch your BurstIO credits in CloudWatch, especially if you have a large number of clients!

EFS Performance

Recommended mount option

`rsize=1M, wsize=1M`

Smaller values limit throughput for large files

Use EFS mount helper to automatically use recommended mount options

Parallelize filesystem access

Up to 40 concurrent transfers per client

2-3 instances can exhaust the IOPS of a General Purpose filesystem

Always test your throughput, don't assume you can achieve the maximum!

DEMO

Create EFS file system

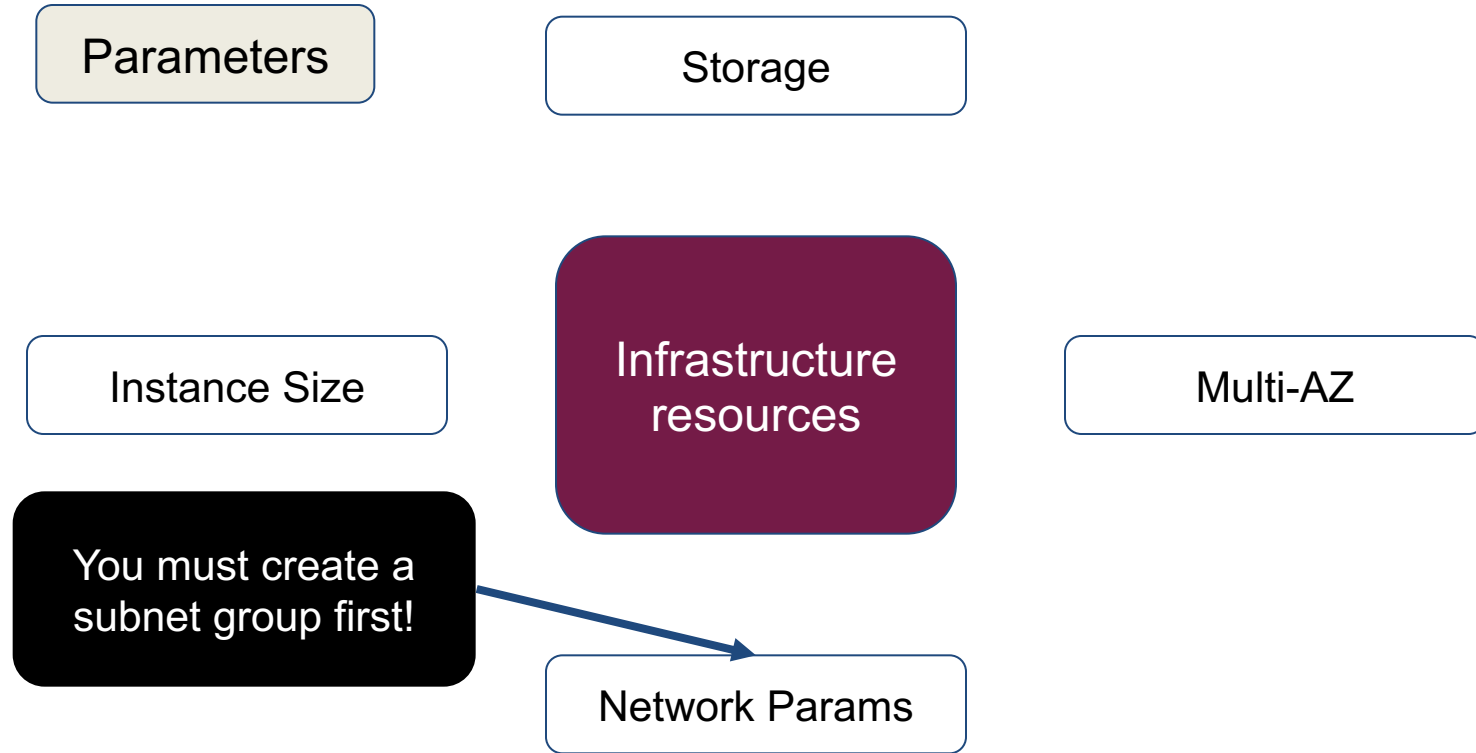
Create mount point in VPC

Mount file system on EC2 instance

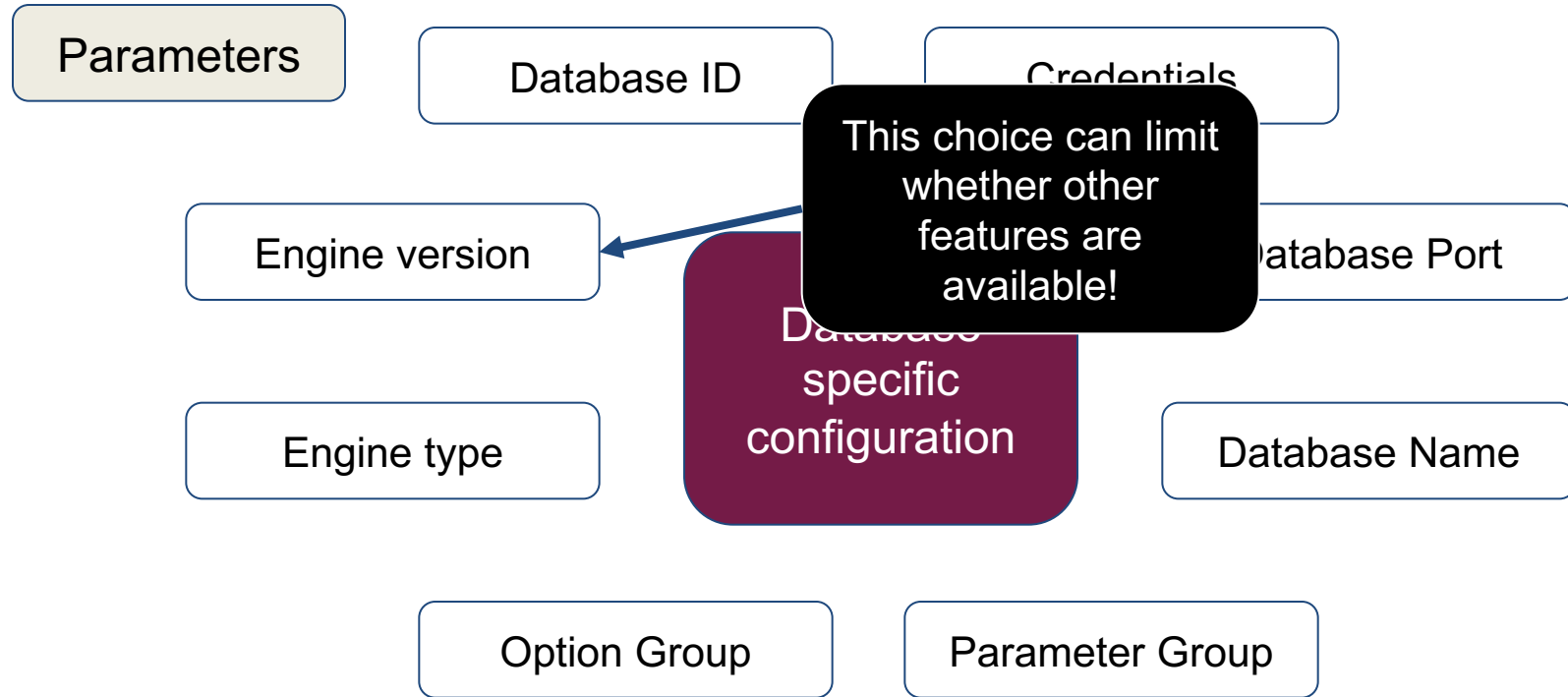


Deploying and Managing RDS

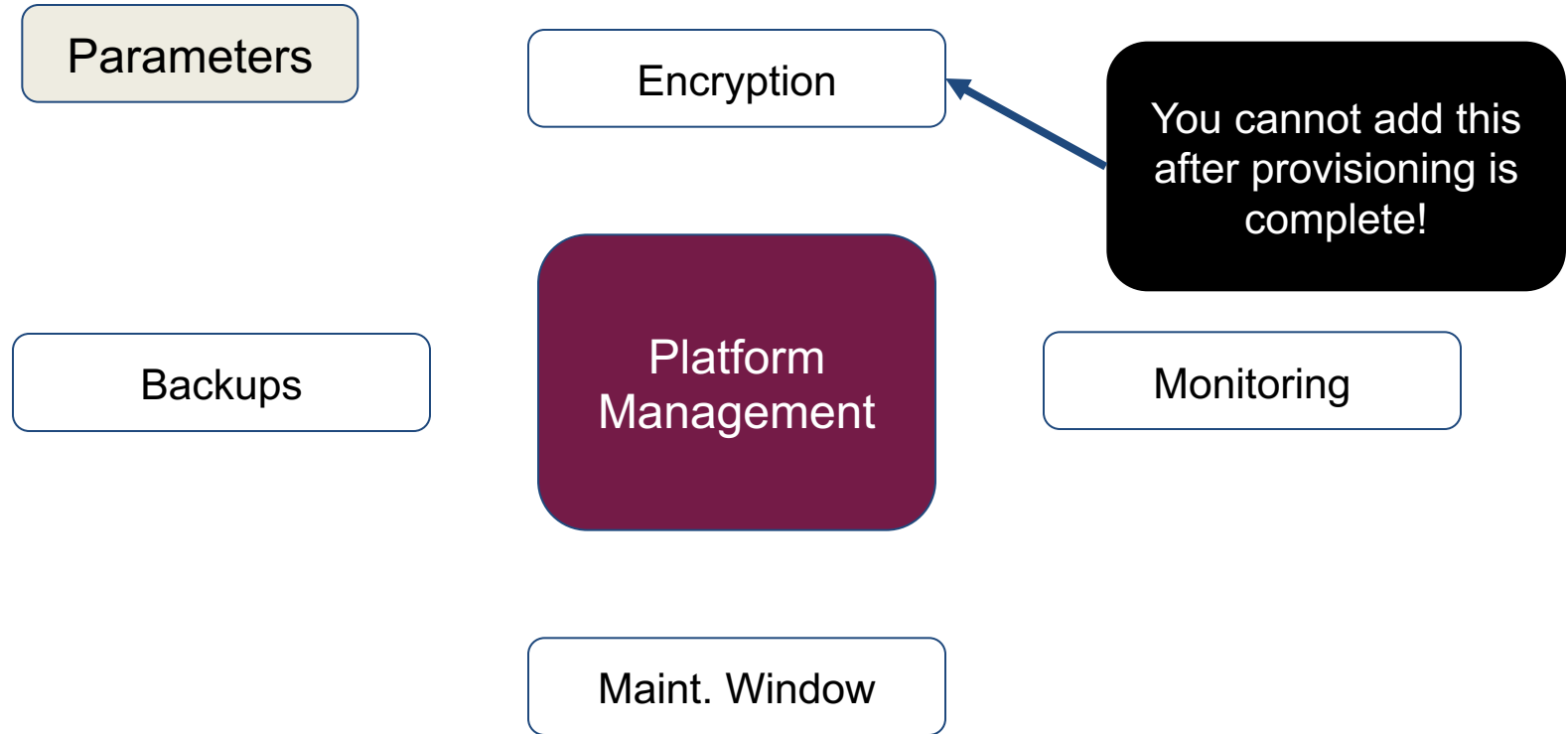
RDS Provisioning 1 of 3



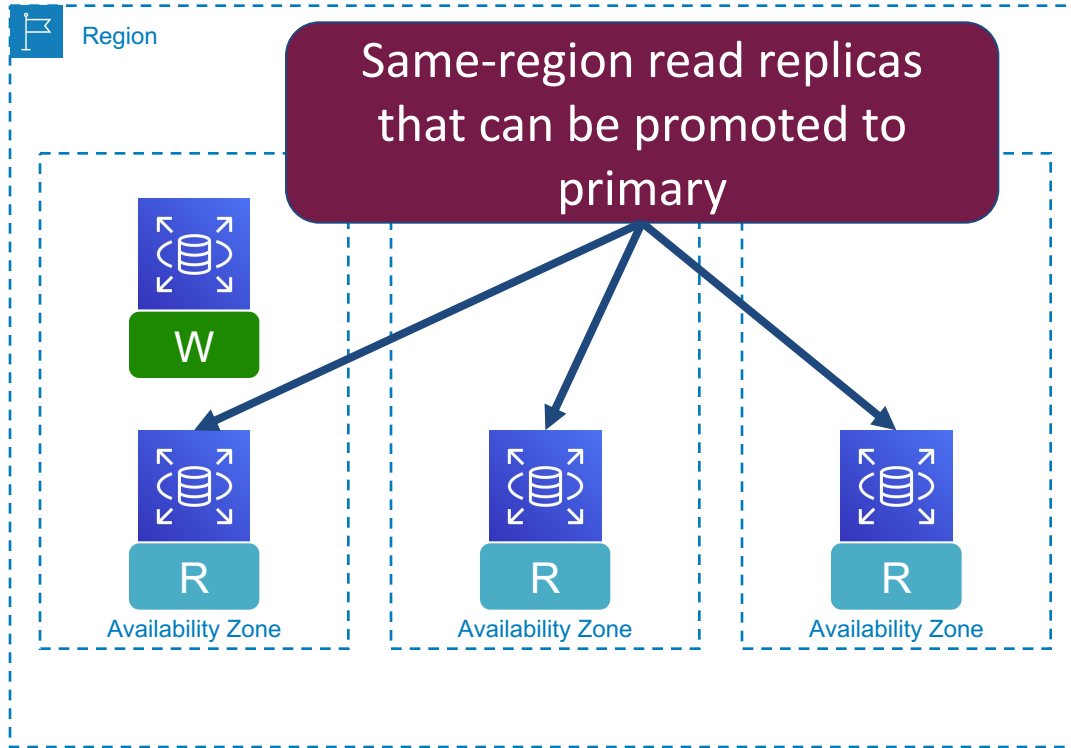
RDS Provisioning 2 of 3



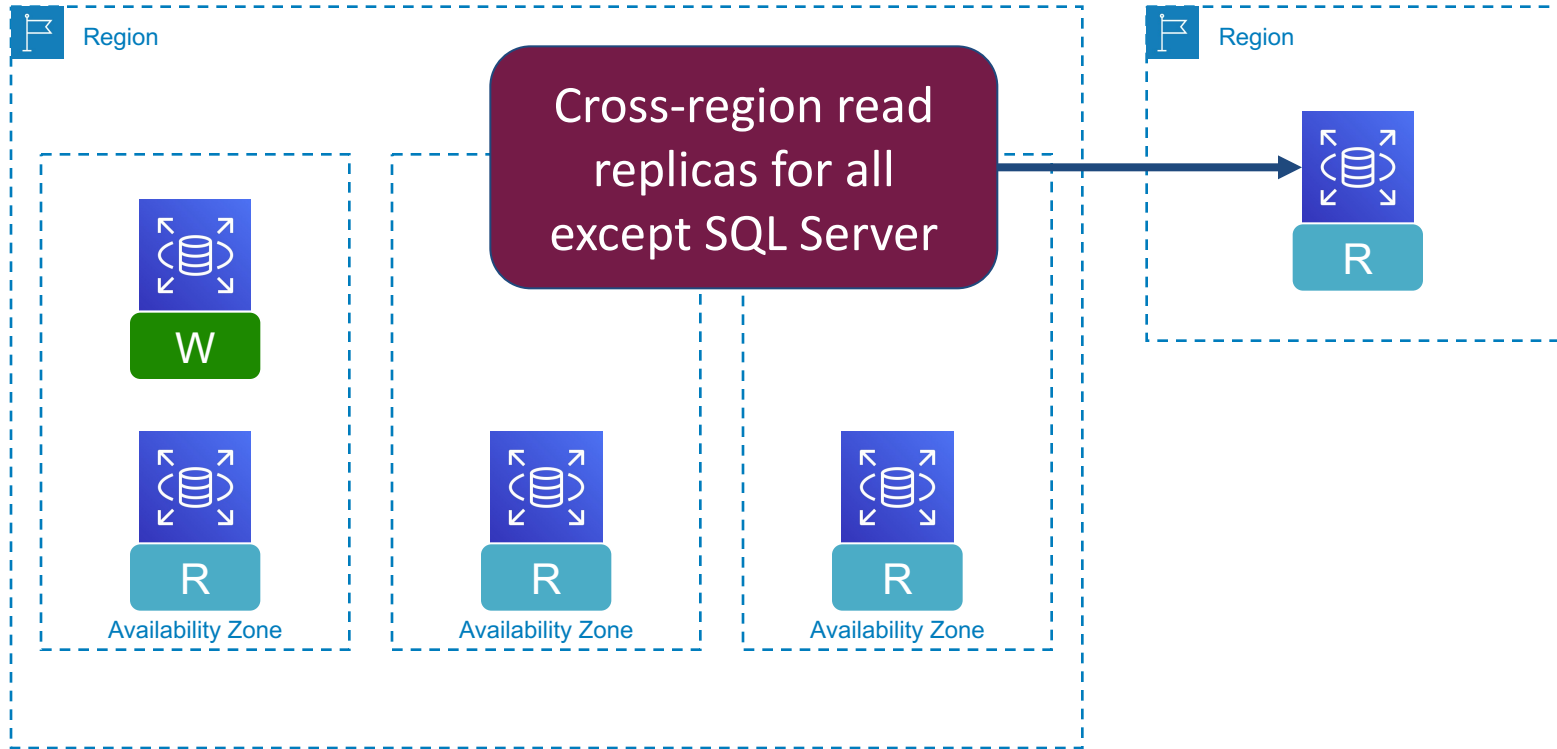
RDS Provisioning 3 of 3



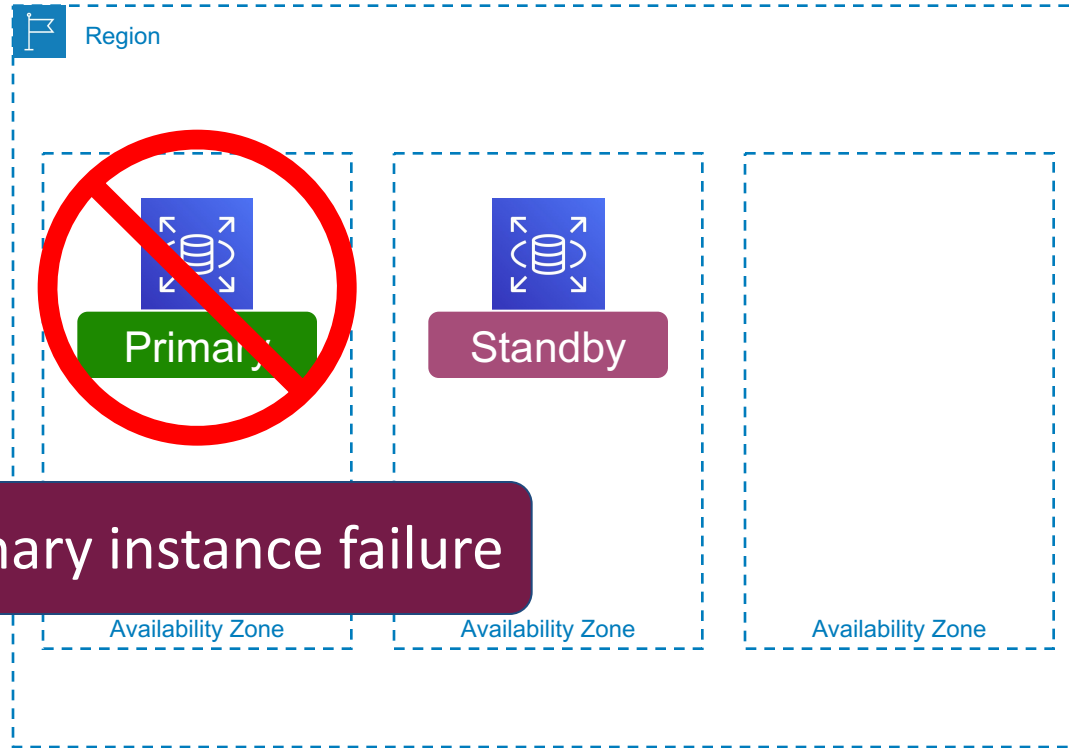
RDS Resilience



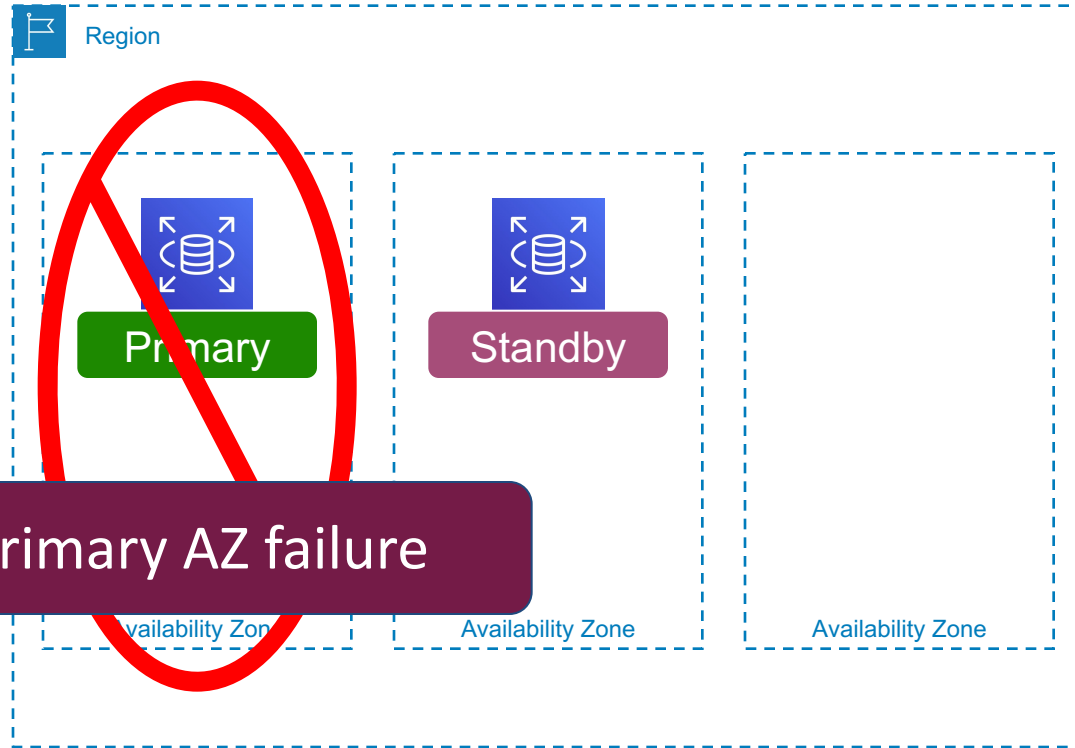
RDS Resilience



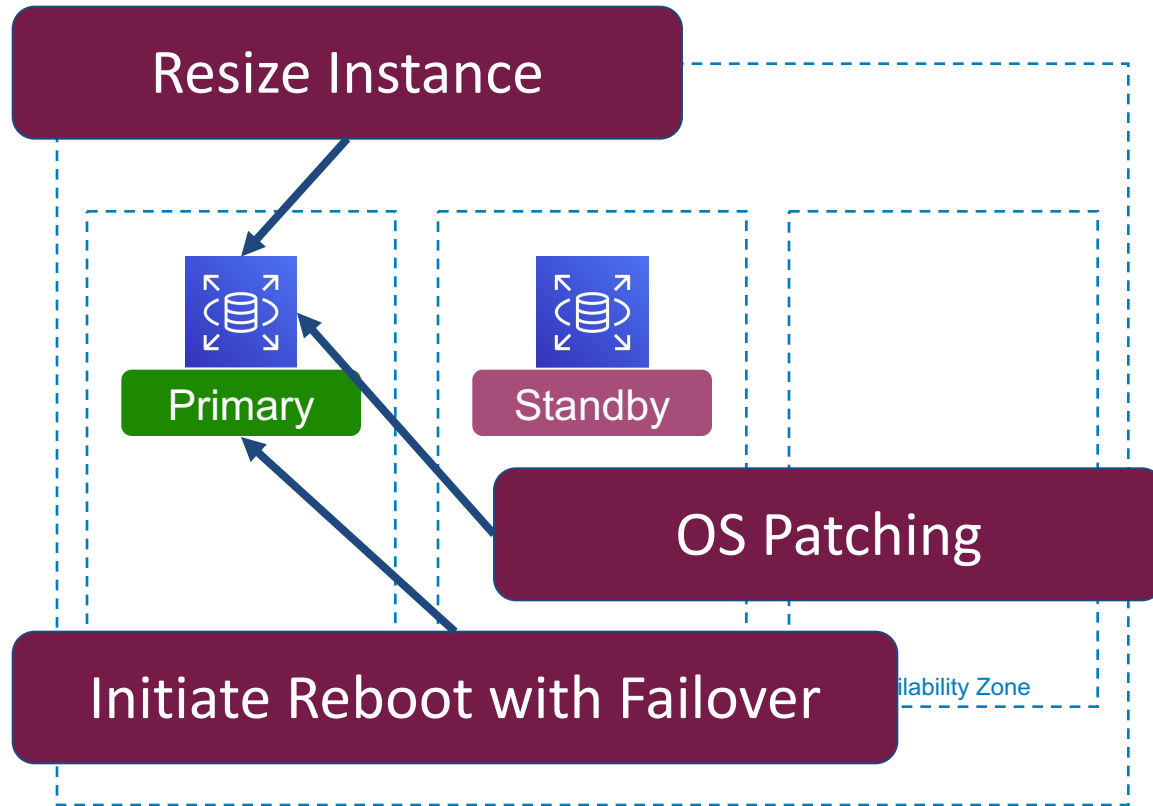
RDS Multi-AZ Failover Conditions



RDS Multi-AZ Failover Conditions



RDS Multi-AZ Failover Conditions



Scenario

A DBA needs to configure **lower_case_table_names=1** for an RDS database instance running MySQL 5.6. How can this task be accomplished?

RDS Default Parameter Group



default.mysql5.6

Oops! Can't edit
this!

Check which
parameter group
is associated

RDS Parameter Group Creation



default.mysql5.6

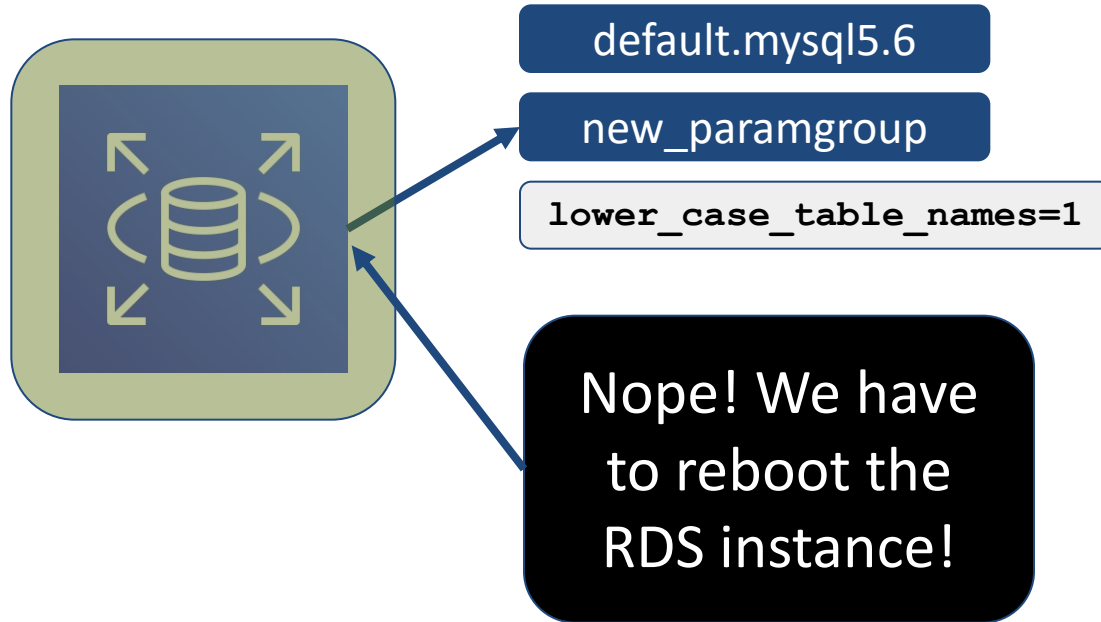
new_paramgroup

`lower_case_table_names=1`

Create and
modify a new
parameter group

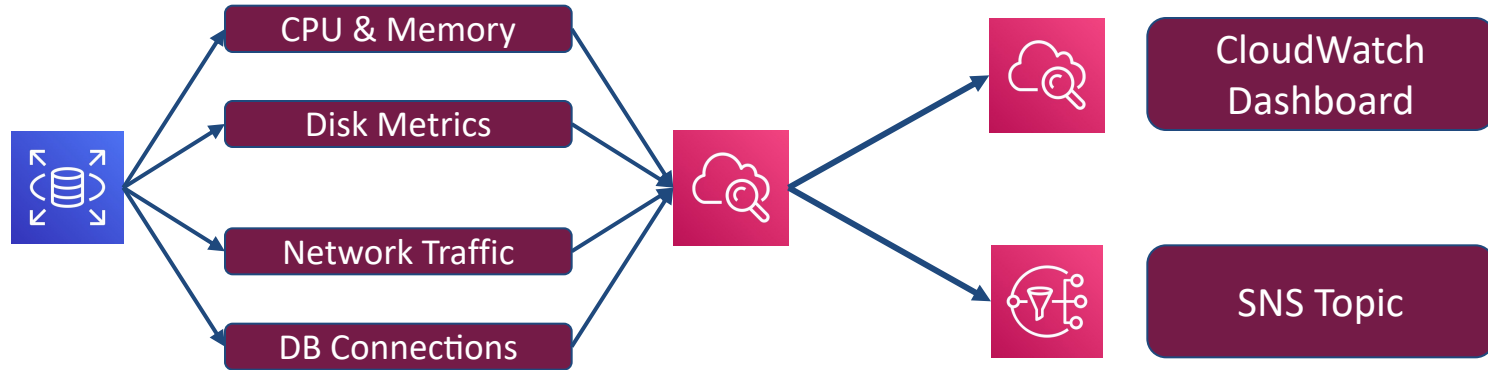
Associate the
new parameter
group with RDS

RDS Parameter Group Effects



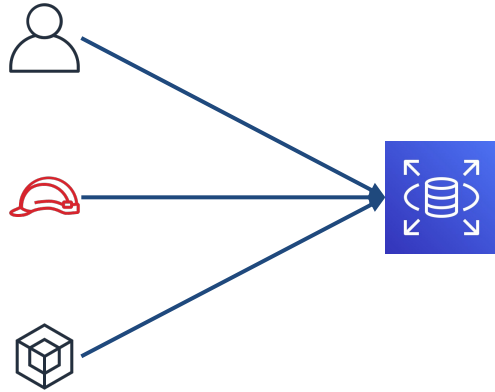
We should be done, right?

CloudWatch Metrics/Alarms



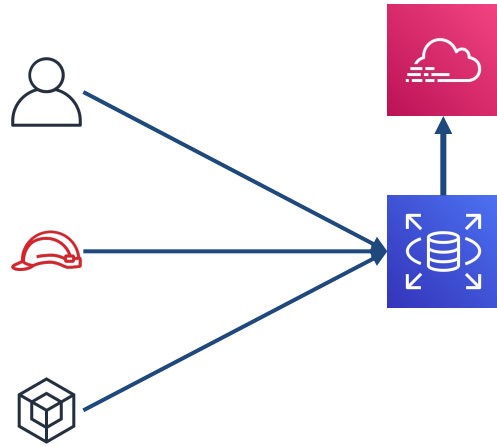
All metrics are gathered from the hypervisor perspective

CloudTrail Logging



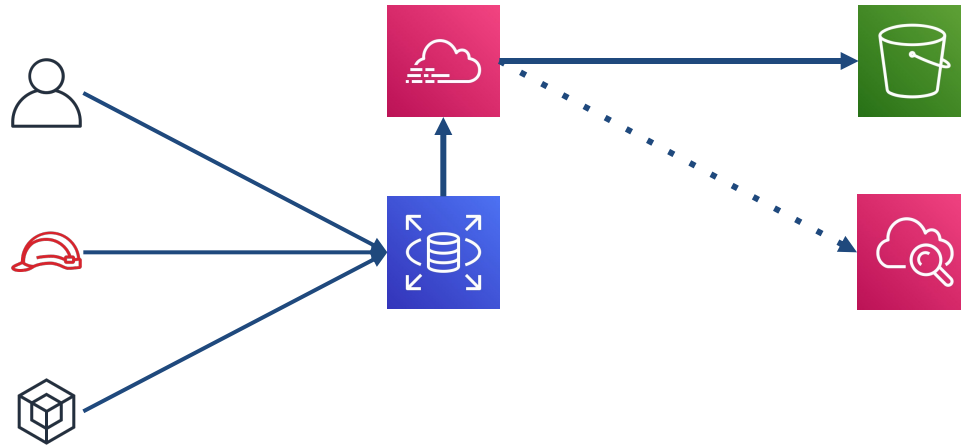
IAM Users, Roles and
other services invoke
RDS actions

CloudTrail Logging



All RDS actions are
logged to CloudTrail,
successful or not

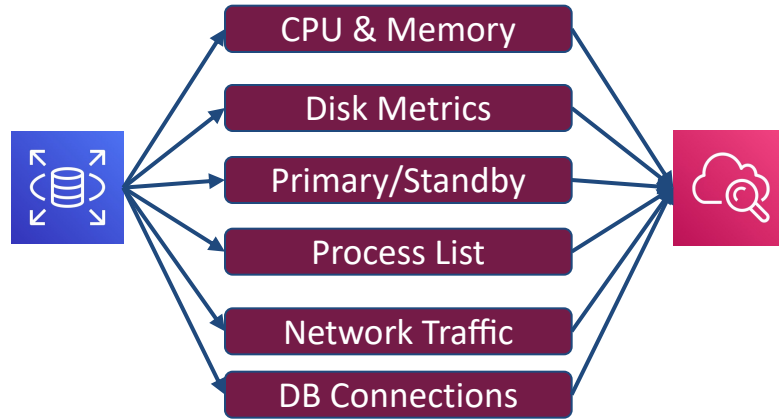
CloudTrail Logging



RDS log entries are delivered to S3 by default, optional to CloudWatch Logs

CloudWatch Logs metric filters can be used to generate metrics, graphs, and CloudWatch Alarms

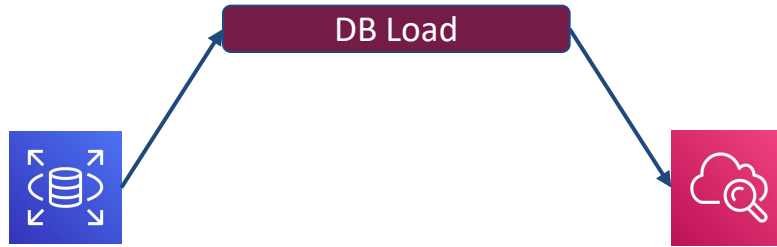
Enhanced Monitoring



Fine-grained, real-time metrics are gathered from the OS perspective and stored in CloudWatch Logs

OS metrics are different for SQL Server instances than for the other engines

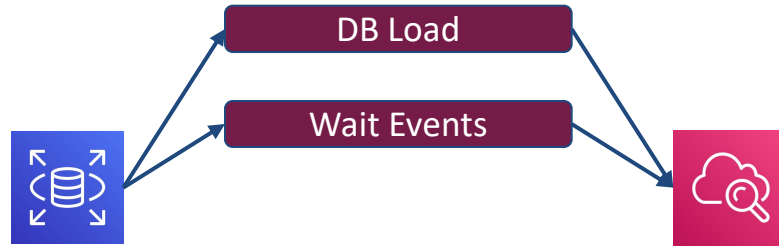
Performance Insights



Performance Insights are enabled upon creation or by modifying an existing database instance and published to CloudWatch as metrics

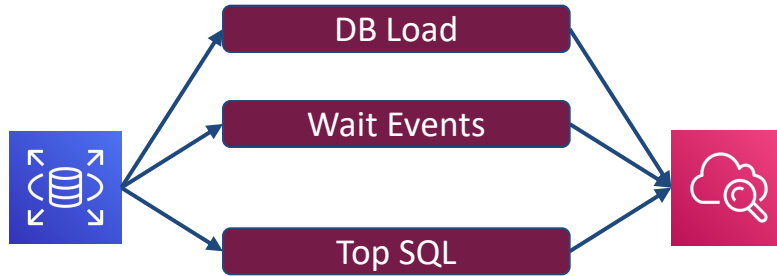
DB Load is the number of active sessions

Performance Insights



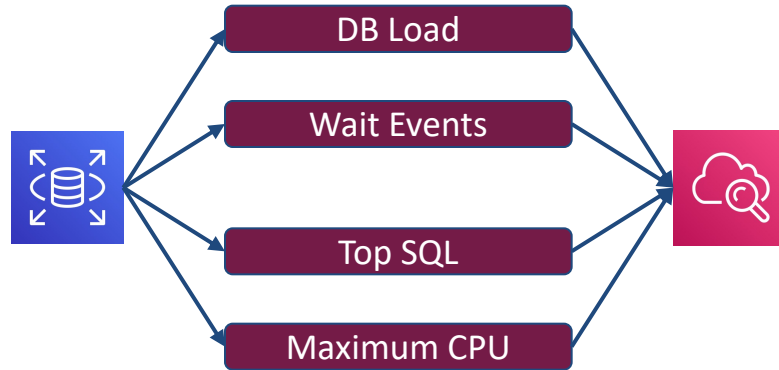
Wait events are unique
to each database engine

Performance Insights



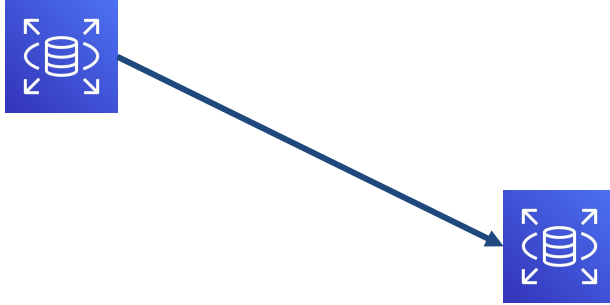
Top SQL shows which queries contribute most to DB load

Performance Insights



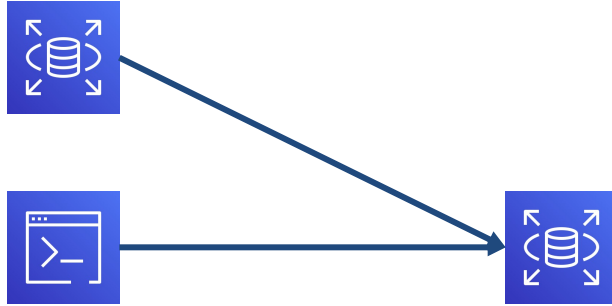
Max CPU is determined
by the number of vCPU
for the instance

Database Logs



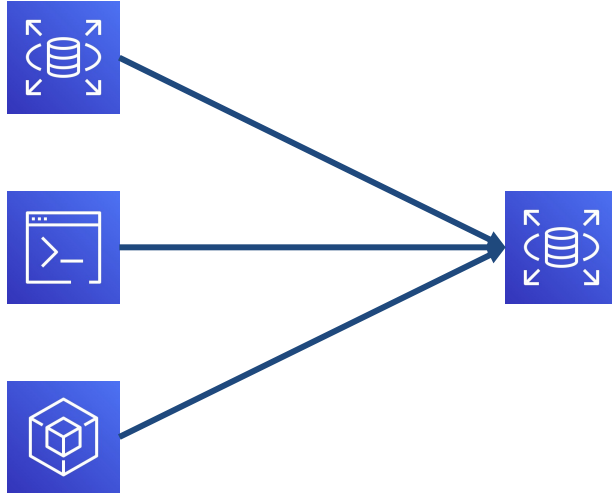
Use the RDS Dashboard in the AWS console to view the various database logs

Database Logs



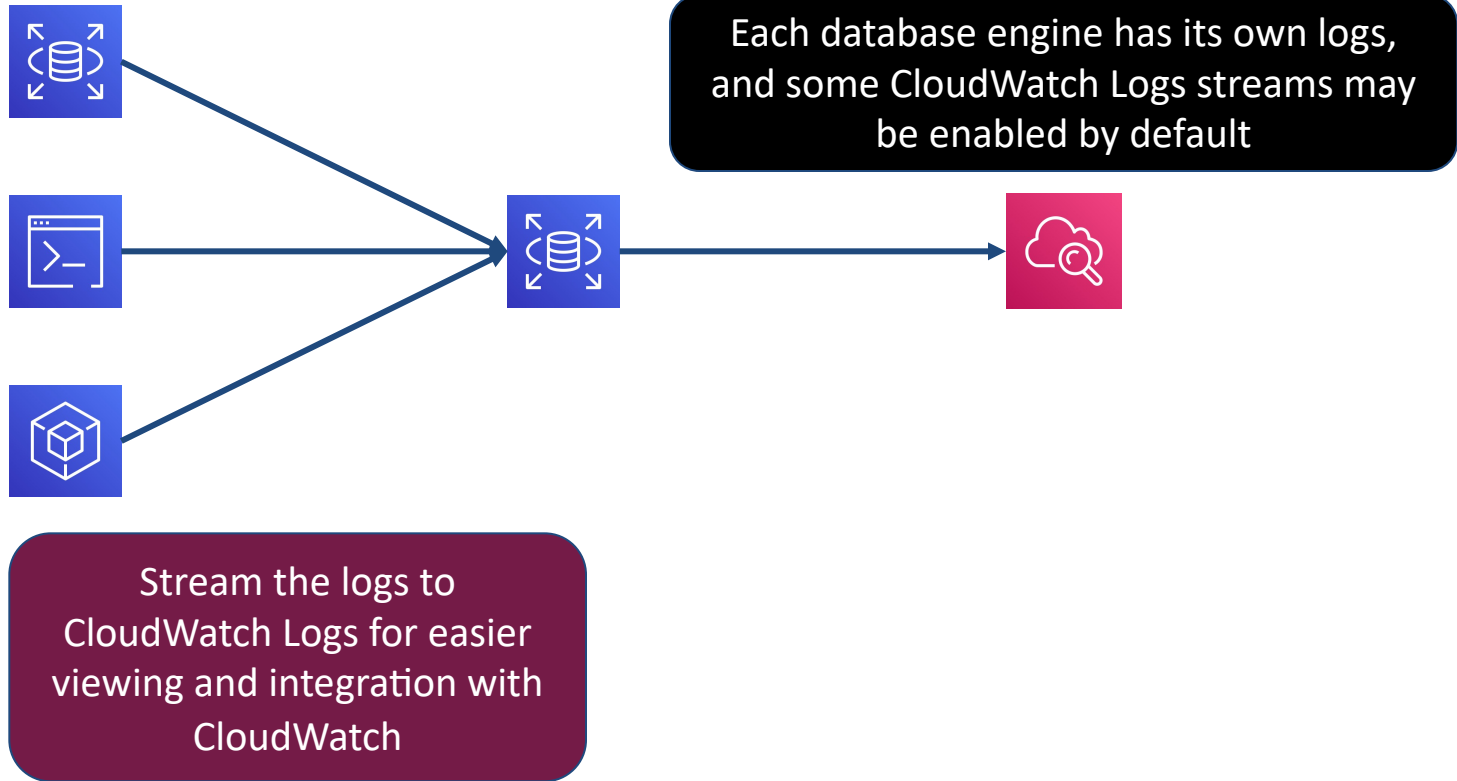
Use the AWS CLI to export
logs for local viewing

Database Logs

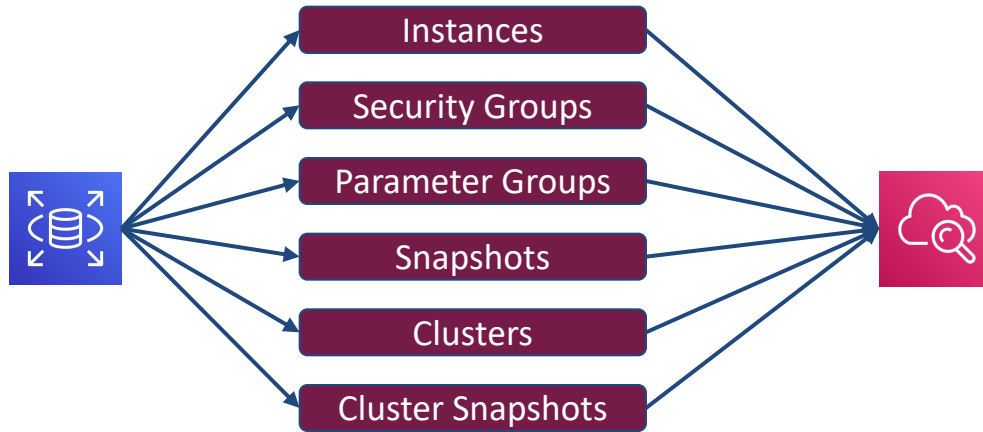


Use the AWS language SDKs
to export logs for local
viewing

Database Logs



Event Notifications



Uses SNS Topics as
destination for RDS events

DB Instance Status

available
backing-up
backtracking
configuring-enhanced-monitoring
configuring-iam-database-auth
configuring-log-exports
converting-to-vpc
creating
deleting
failed
inaccessible-encryption-credentials
incompatible-network
incompatible-option-group
incompatible-parameters

Availability?

Performance?

Durability?

incompatible-restore
maintenance
modifying
moving-to-vpc
rebooting
resizing
setting-master-credentials
storage-error
storage-optimization
storage-full
storage-optimization
upgrading

DEMO

Deploy Aurora using CloudFormation

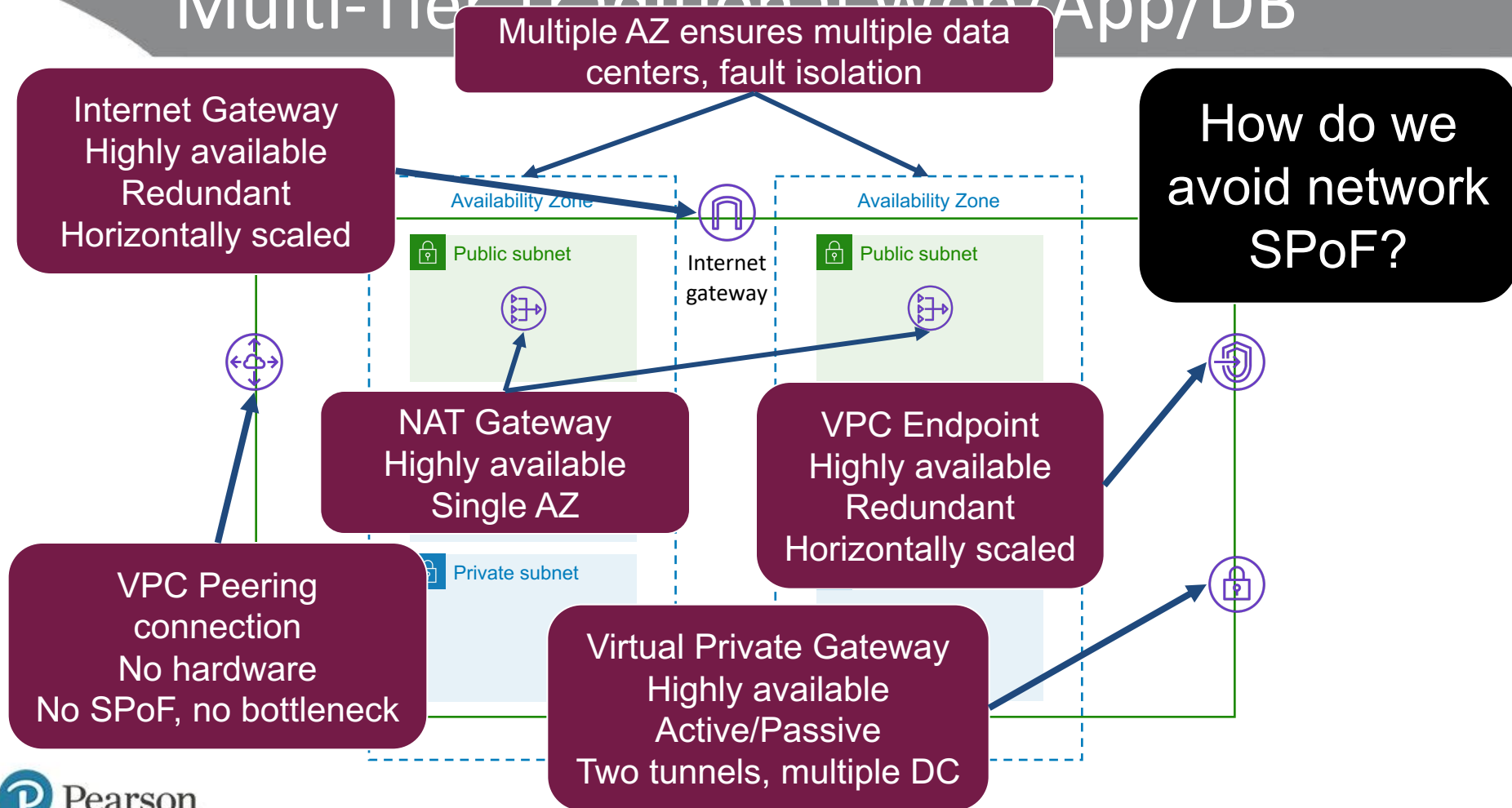
Enable monitoring options

Enable custom parameters



Provisioning 3-tier Architectures

Multi-Tier Traditional Web/App/DB

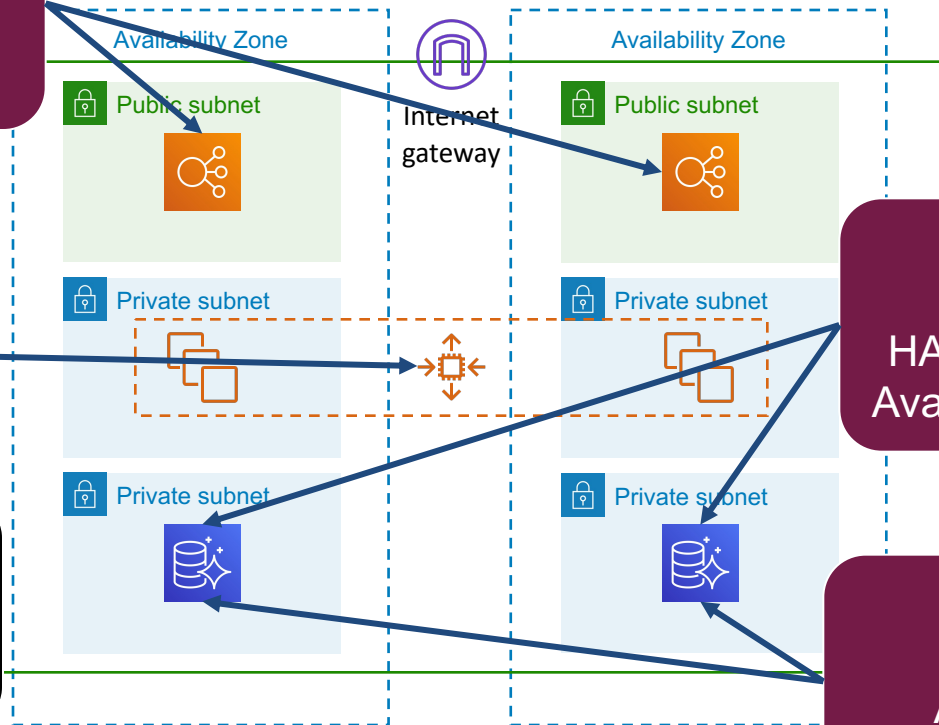


Multi-Tier Traditional Web/App/DB

ELB
Multi-AZ
Redundant
Availability 4 9s

Auto Scaling
Multi-AZ
Redundant (EC2)
Availability 1 9/EC2

Entire infrastructure:
Highly available
Self-healing
Automatic Scaling**
Can we do better?

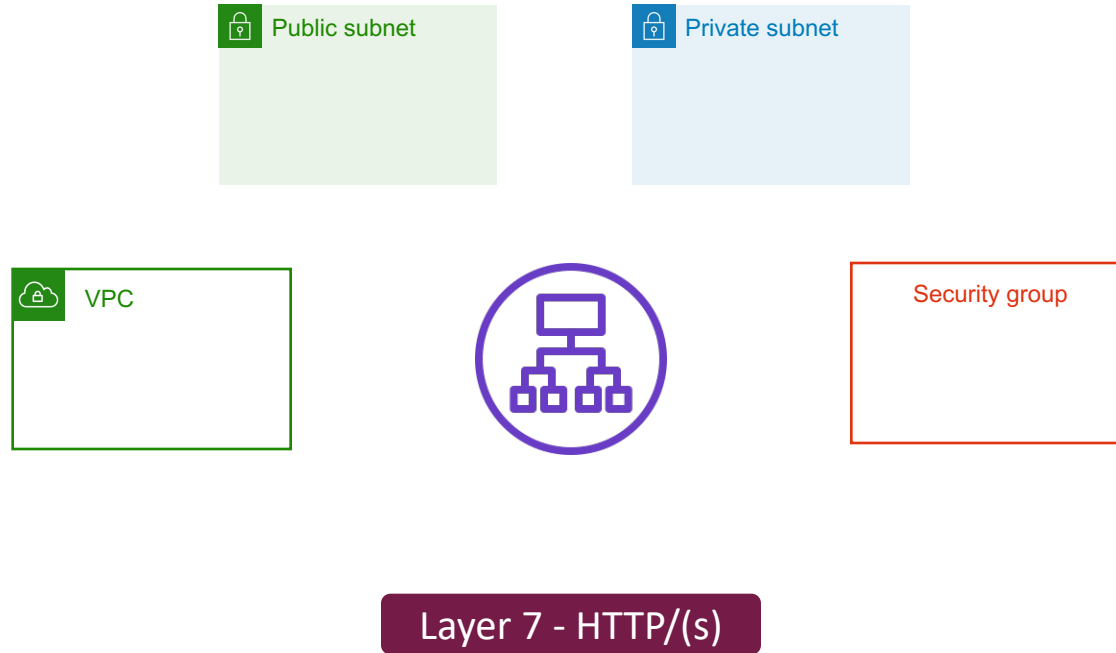


How do we
avoid
application
SPoF?

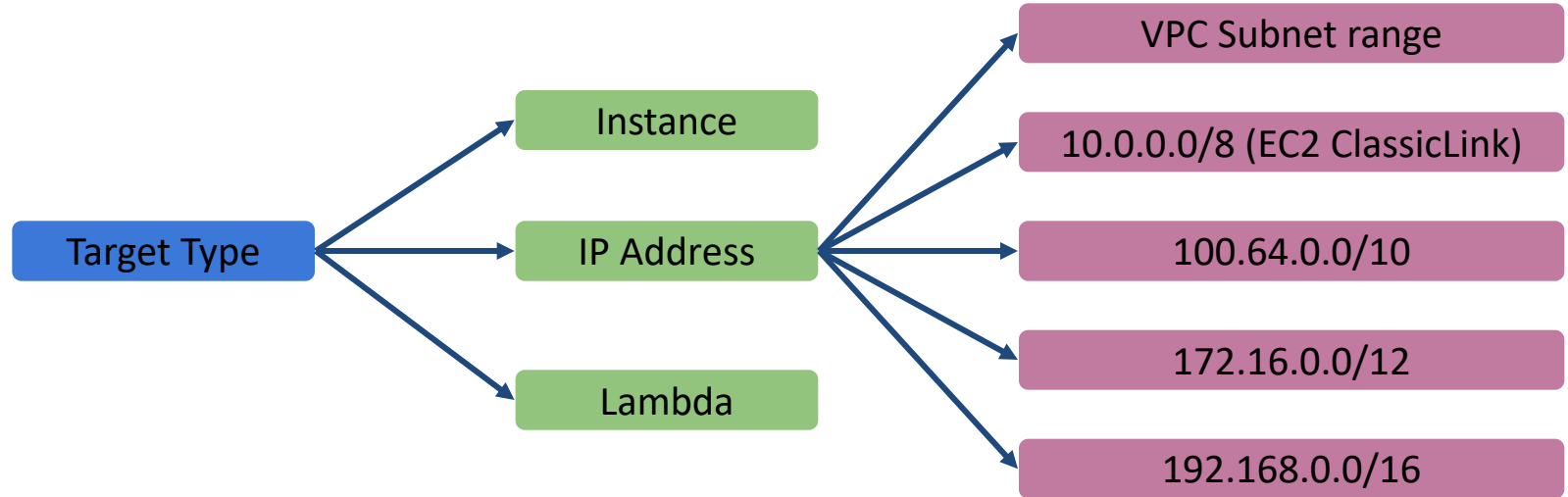
RDS/Aurora
Multi-AZ
HA - active/passive writes
Availability 3.5 9s/Node OR

Aurora
Multi-Primary
Active/active writes
Availability 4 9s

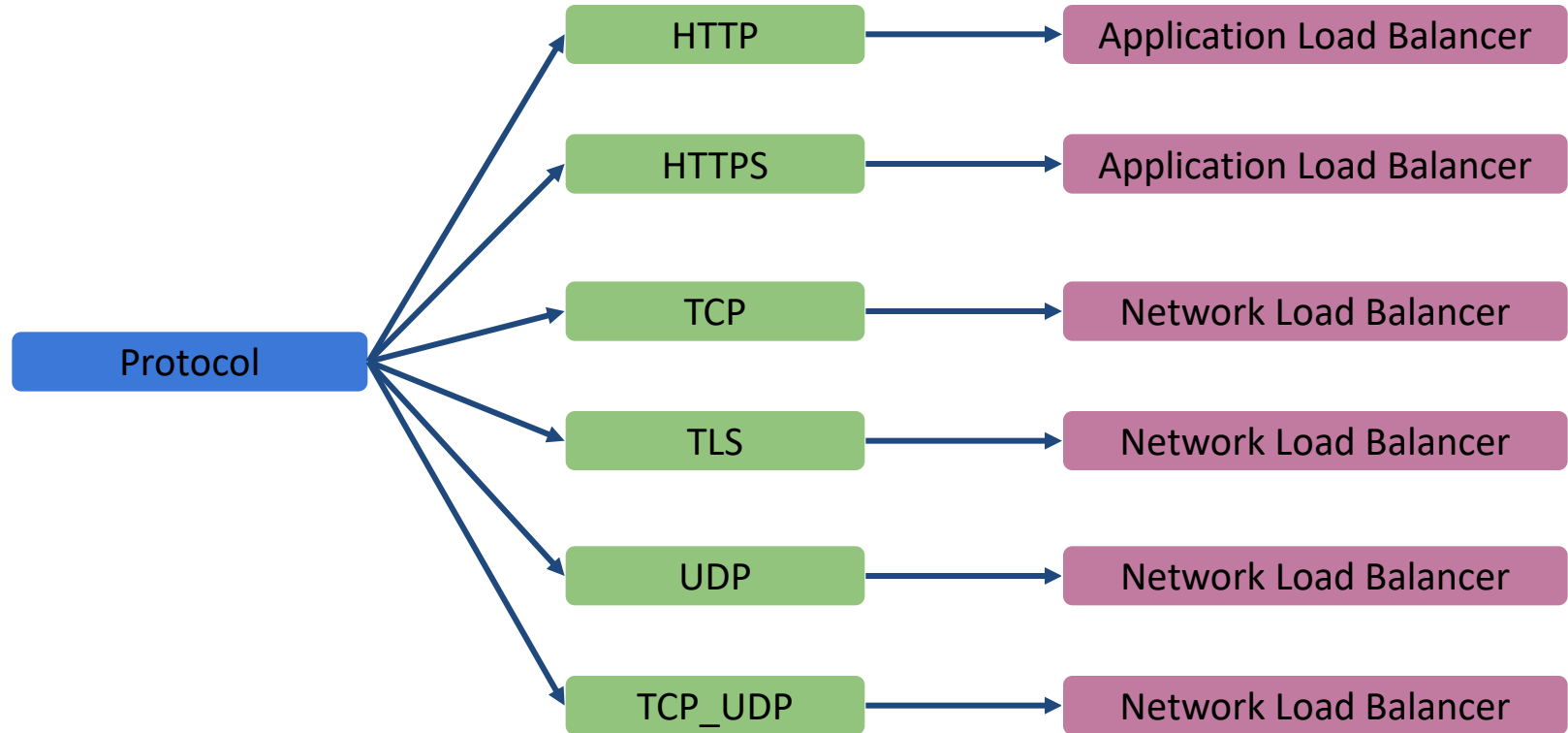
Application Load Balancer



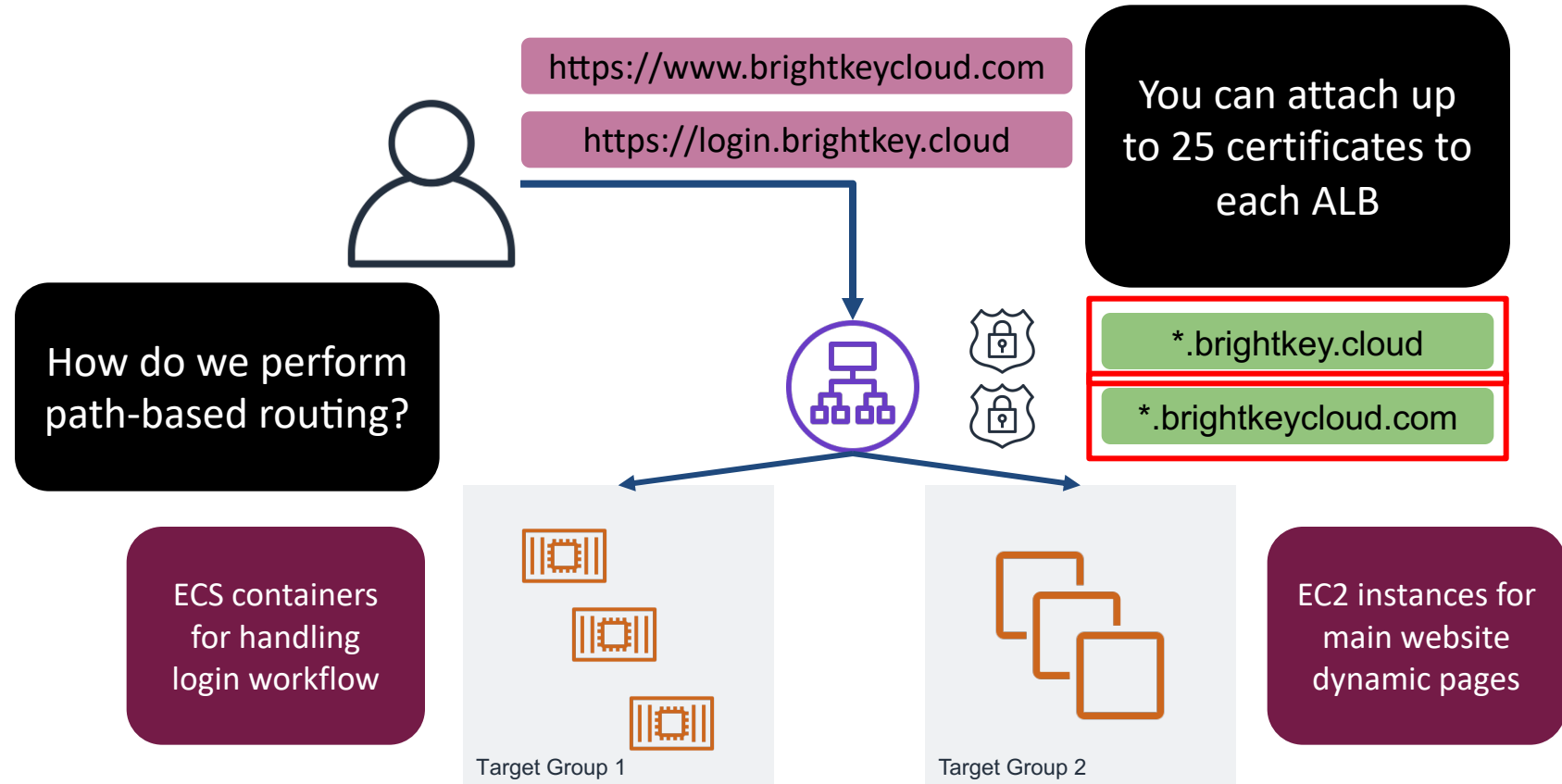
Target Group Configuration



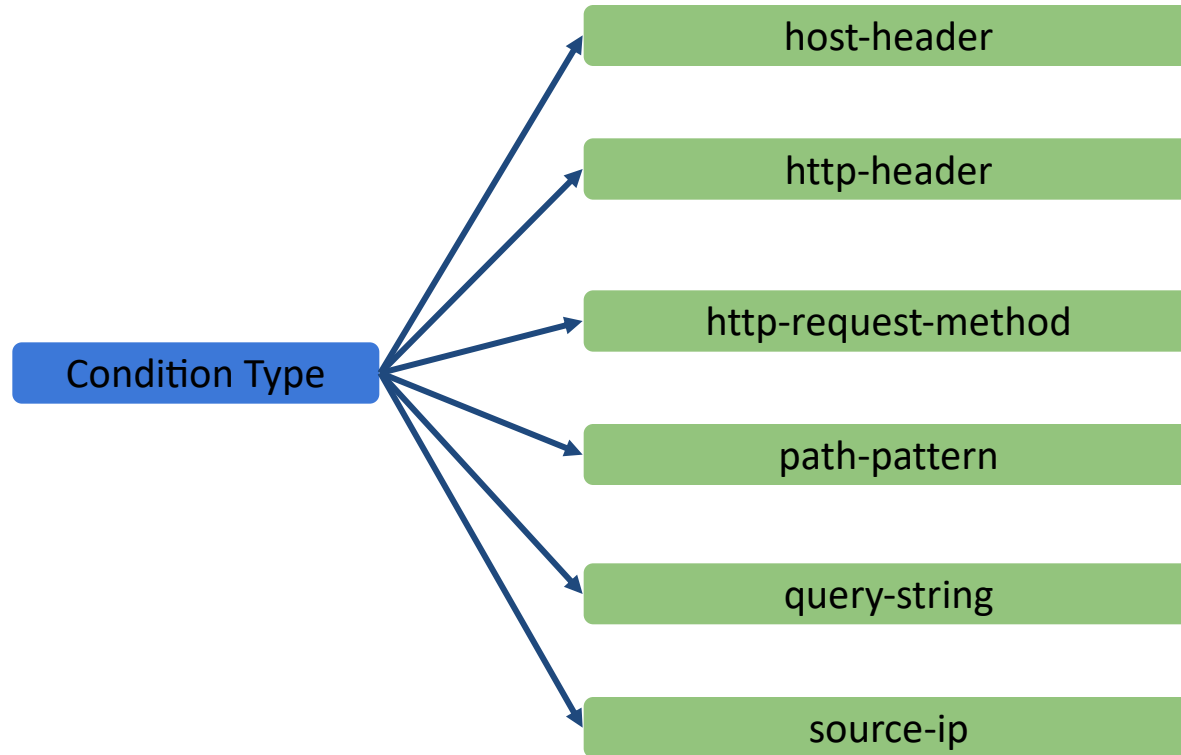
Target Group Configuration



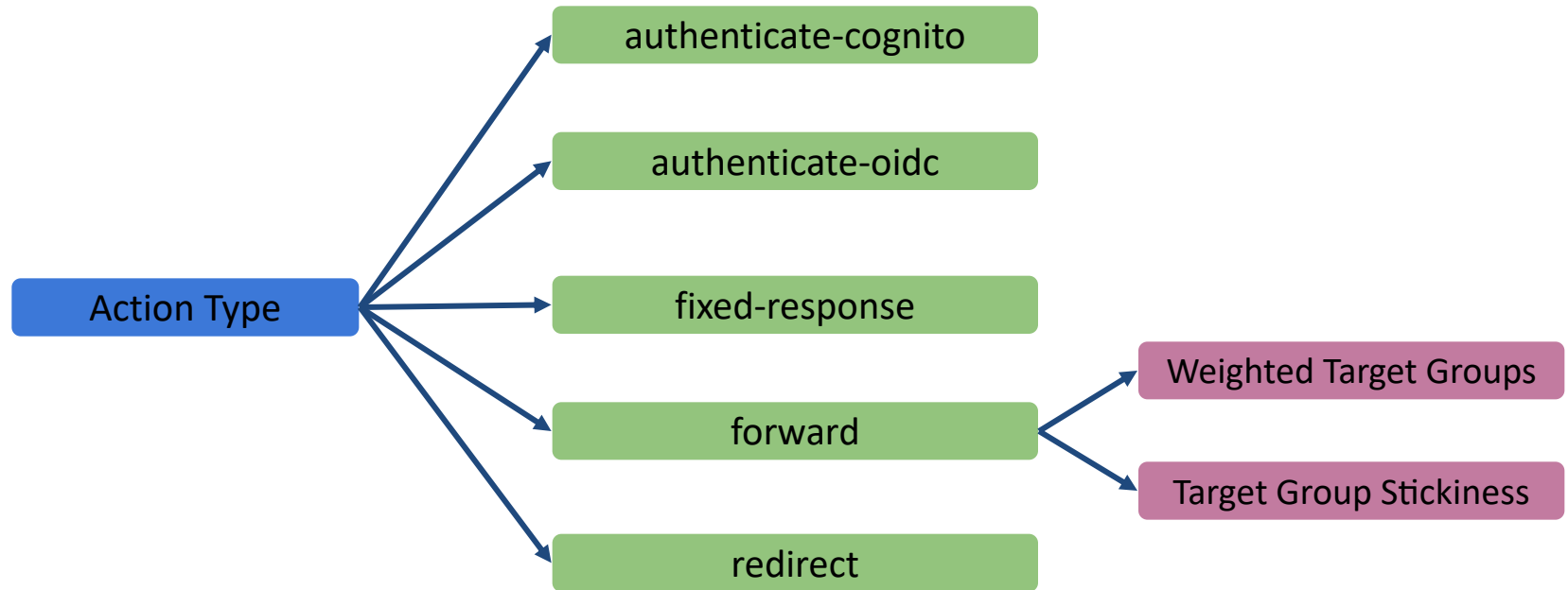
ALB TLS Certificate Smart Selection



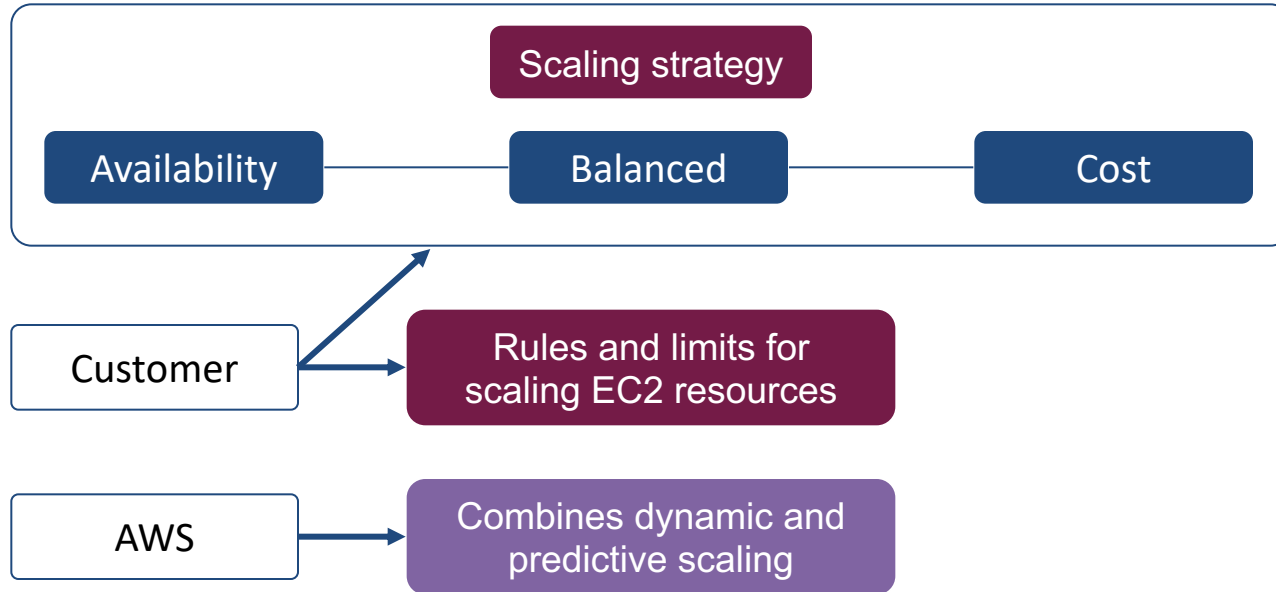
ALB Listener Rules



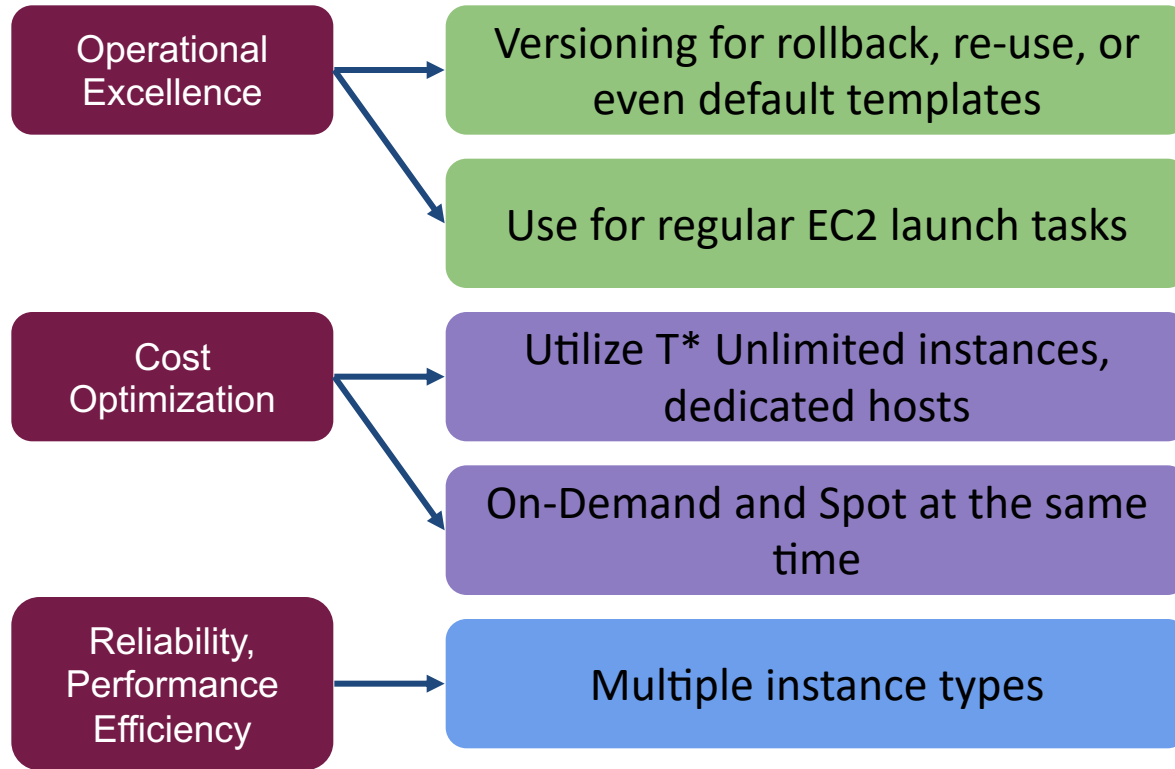
ALB Listener Rules



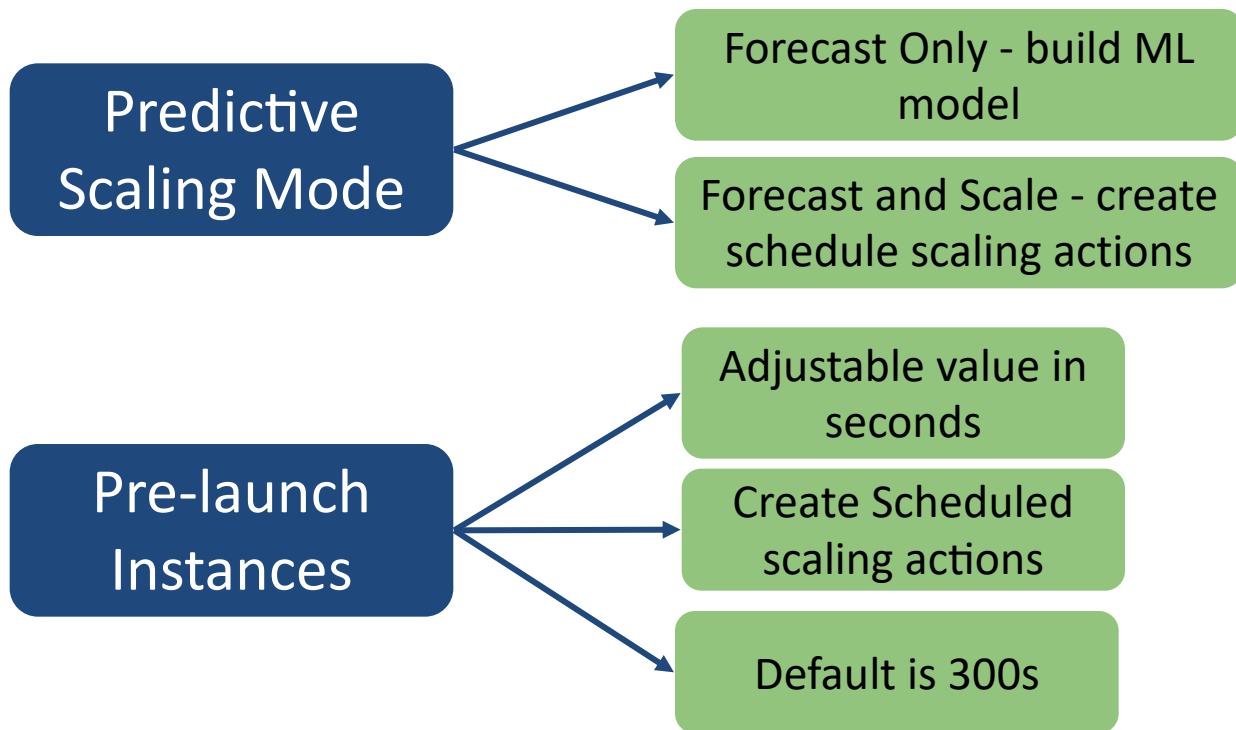
What is a Scaling Plan for EC2?



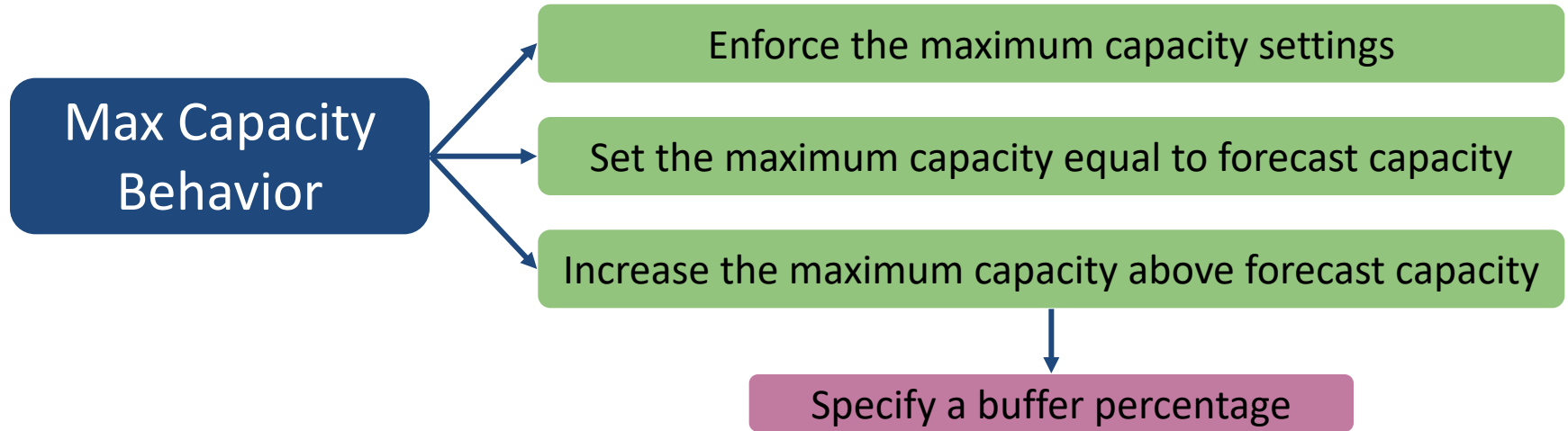
What is a Launch Template?



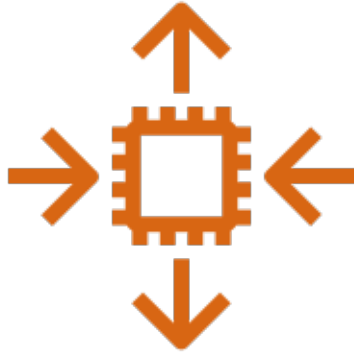
What is Predictive Scaling?



Predictive Scaling Options



Auto Scaling Operations



Auto Scaling policies

Monitor ASG limits

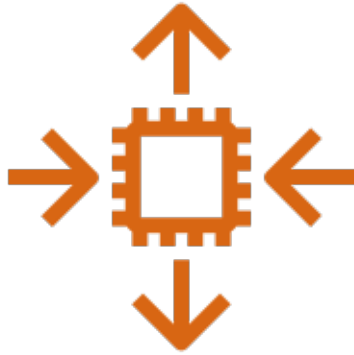
Deploy launch templates

Lifecycle hooks

Cooldown periods

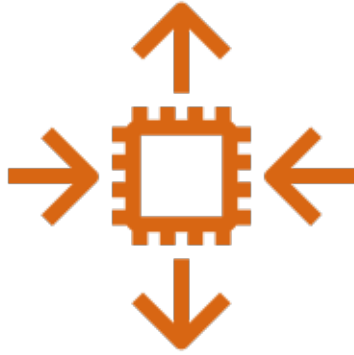
Warm Pool configuration

Auto Scaling Scenarios



Stateless web apps
Unpredictable traffic
Steady-state groups
Message consumer apps

Auto Scaling Anti-Scenarios



Monolithic applications
(singleton instance)

Applications with fixed IP
addresses

Applications with many
manual deploy steps

Applications with short,
large, random traffic
spikes

DEMO

Deploy ALB (CLI)

Deploy Auto-scaling Group (Console)

Deploy Secret for RDS connection (Console)



Deploying Static Websites

Static Website Hosting Basics



Enables DNS CNAME pointers

Or use S3 website endpoint

Configure index document

Configure error pages

Configure redirects

Configure access logs

Cannot be used with OAI

No custom TLS

Beware of S3 Block Public Access

S3 Website Endpoints

<http://BUCKETNAME.s3-website-REGION.amazonaws.com>

<http://BUCKETNAME.s3-website.REGION.amazonaws.com>



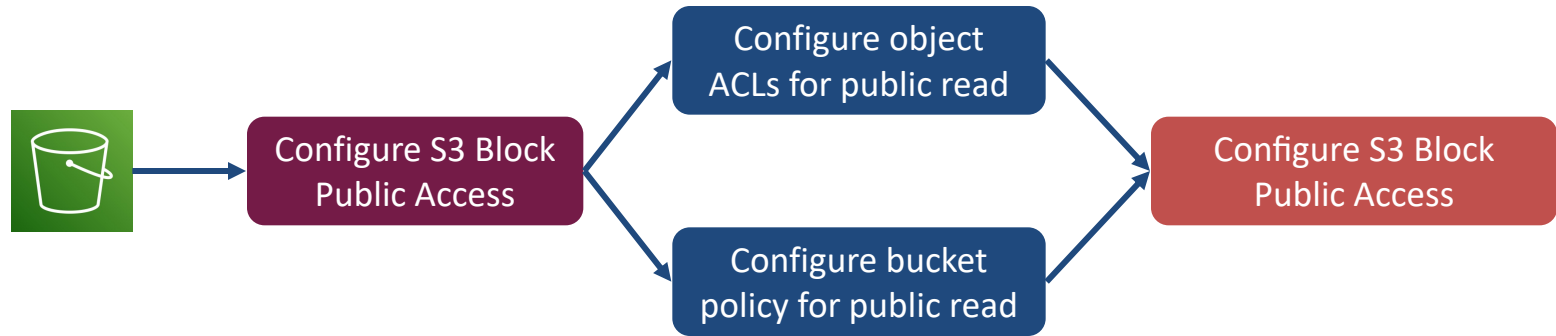
No TLS supported

All resources must be
publicly readable

Only GET and HEAD
requests

Bucket name must
match CNAME FQDN

Static Website Permissions



Static Website Redirect Template

```
[
  {
    "Condition": {
      "HttpErrorCodeReturnedEquals": "string",
      "KeyPrefixEquals": "string"
    },
    "Redirect": {
      "HostName": "string",
      "HttpRedirectCode": "string",
      "Protocol": "http|https",
      "ReplaceKeyPrefixWith": "string",
      "ReplaceKeyWith": "string"
    }
  }
]
```

Static Website Redirect Example 1

```
[
  {
    "Condition": {
      "KeyPrefixEquals": "images/"
    },
    "Redirect": {
      "ReplaceKeyPrefixWith": "img/"
    }
  }
]
```

Static Website Redirect Example 2

```
[
  {
    "Condition": {
      "KeyPrefixEquals": "old_dir/"
    },
    "Redirect": {
      "ReplaceKeyPrefixWith": "deleted.html"
    }
  }
]
```

Static Website Redirect Example 3

```
[  
  {  
    "Redirect": {  
      "HostName": "test.example.com",  
      "ReplaceKeyWith": "http://example.com"  
    }  
  }  
]
```


S3 Origin Access Identity (OAI) Basics

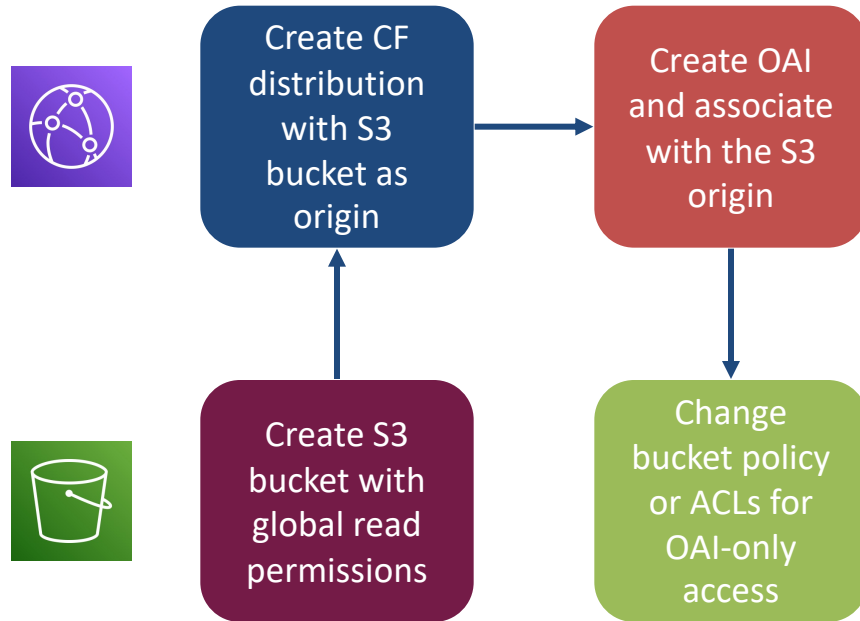


Make S3 resources
private

Must use with
CloudFront

Cannot use with S3
website endpoint

OAI Configuration Workflow



DEMO

Create and configure S3 bucket

Deploy static page to S3

Create and configure CloudFront distribution



Implementing Backups

AWS Backup Resources

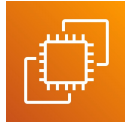


Backup vault
Backup plan
Backup job
Restore point

AWS Backup Supported Services



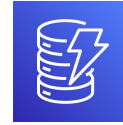
FSx file system



EC2 AMI



EFS file system



DynamoDB table



EBS snapshot



RDS/Aurora
instance



Storage Gateway
snapshots

AWS Backup Workflow

Resource



tag backup:true

Resource assignments
for Backup plans
require tags to function

AWS Backup Workflow

Resource



tag backup:true

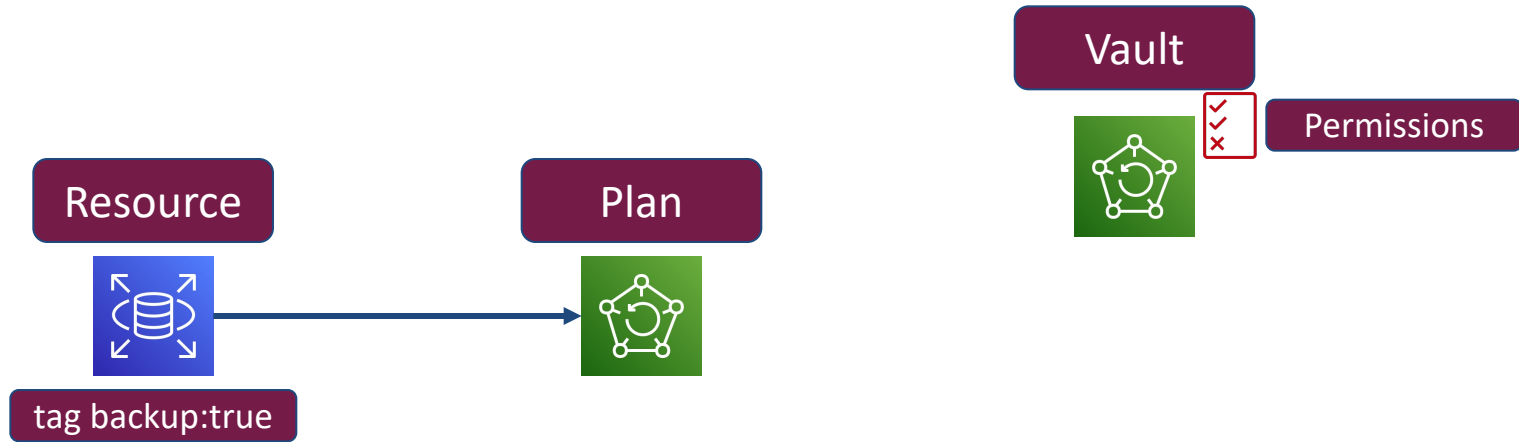
Vault



Permissions

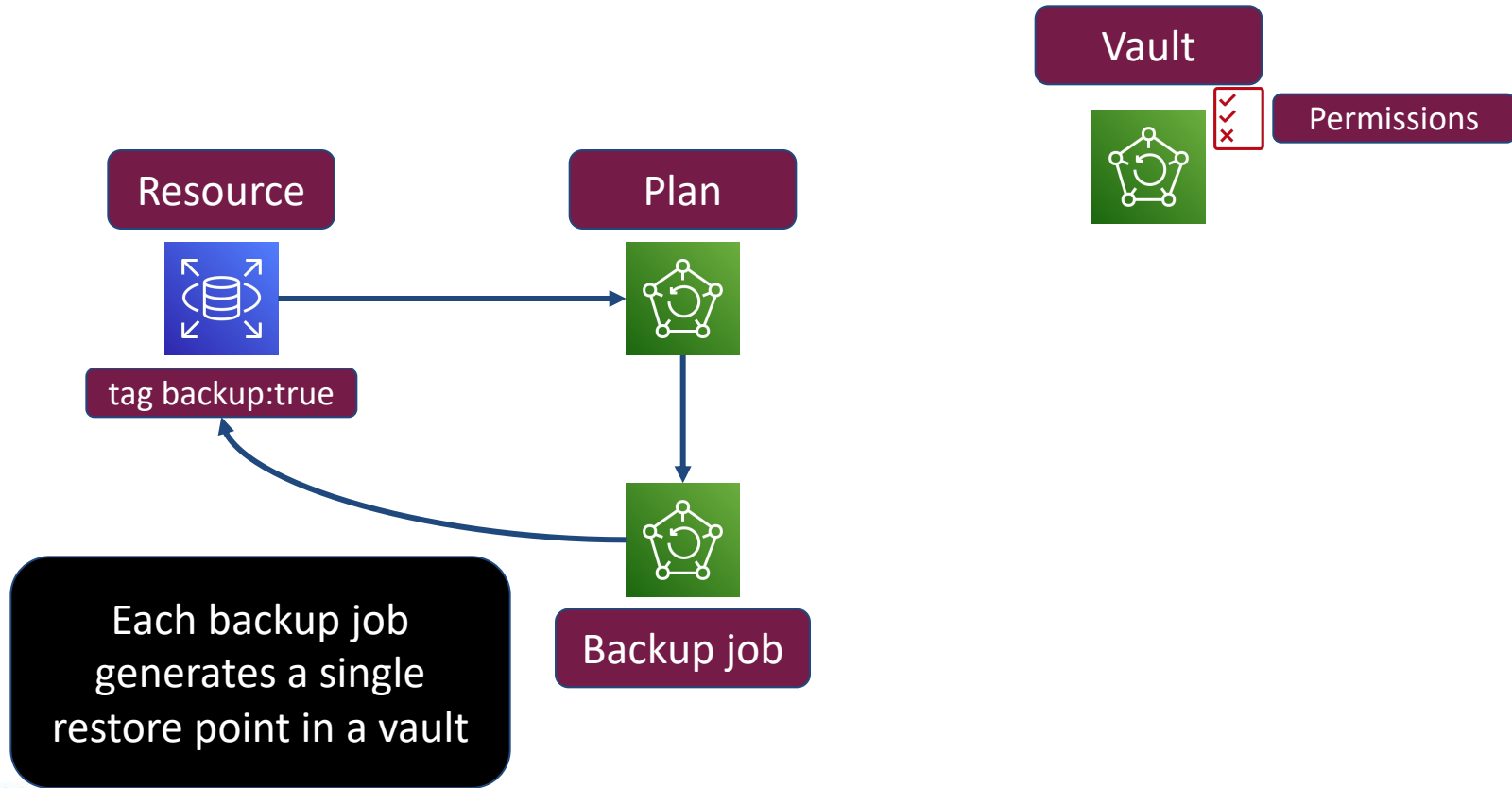
Backup vaults hold
restore points and
provide resource-level
access control

AWS Backup Workflow

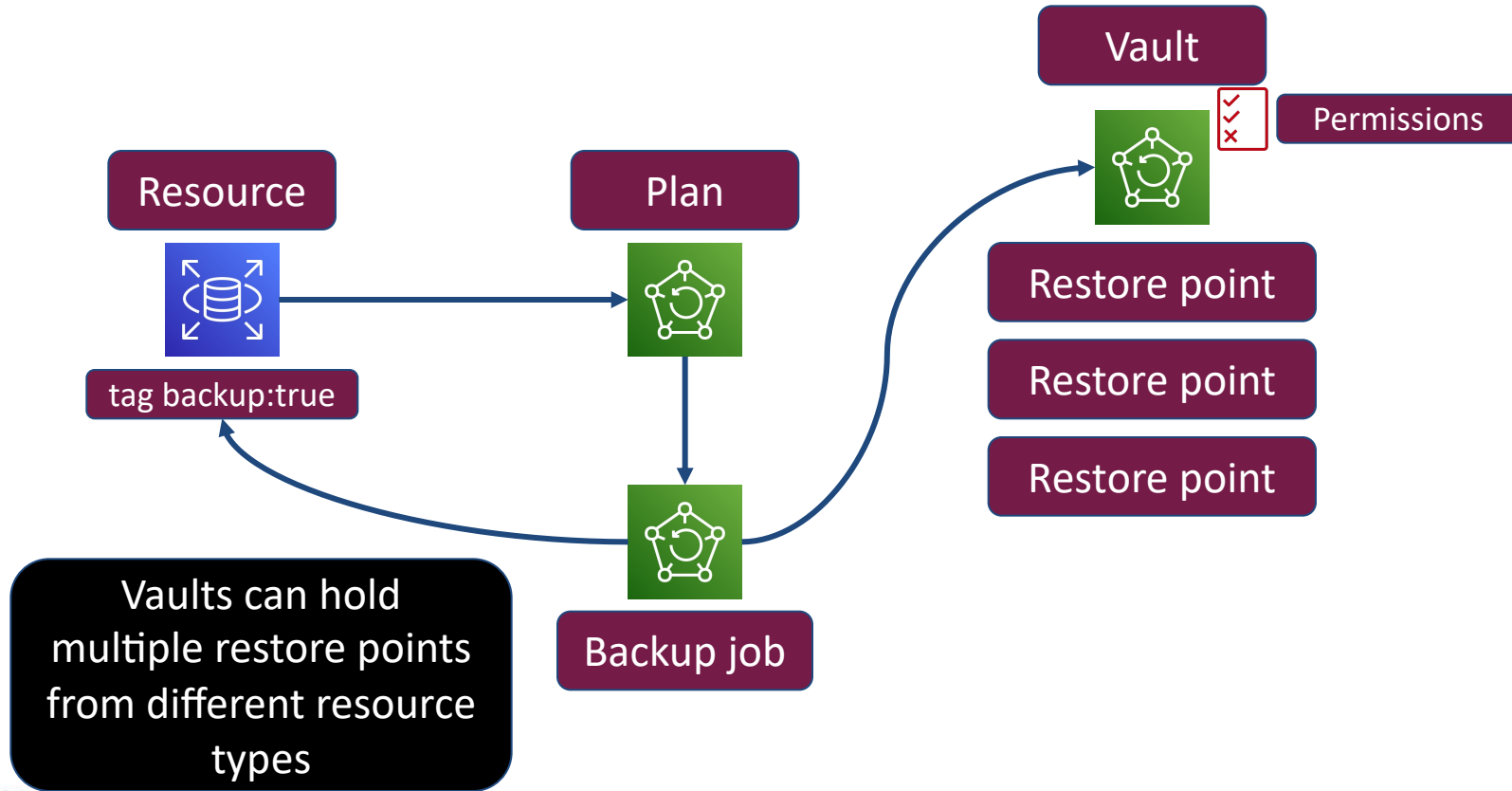


Backup plans provide the integration between resources, jobs and vaults

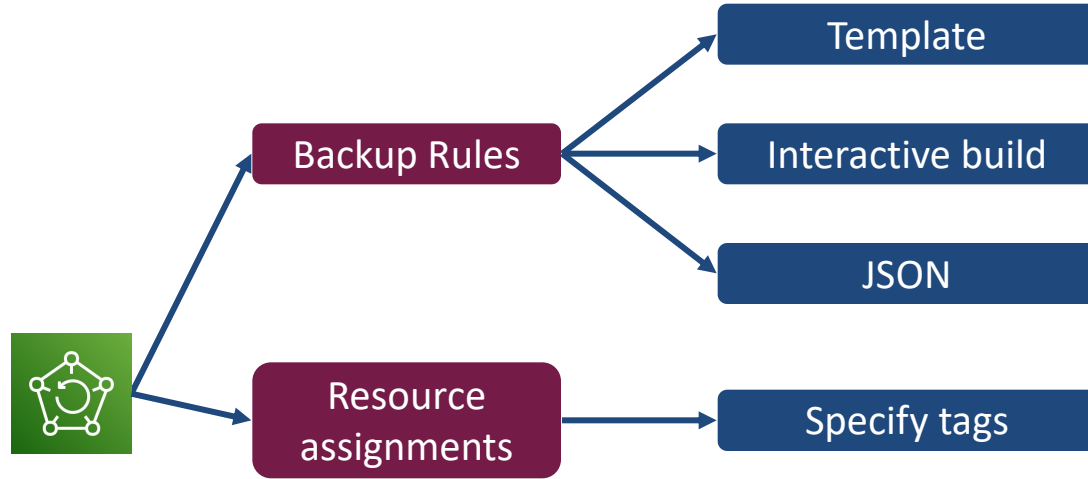
AWS Backup Workflow



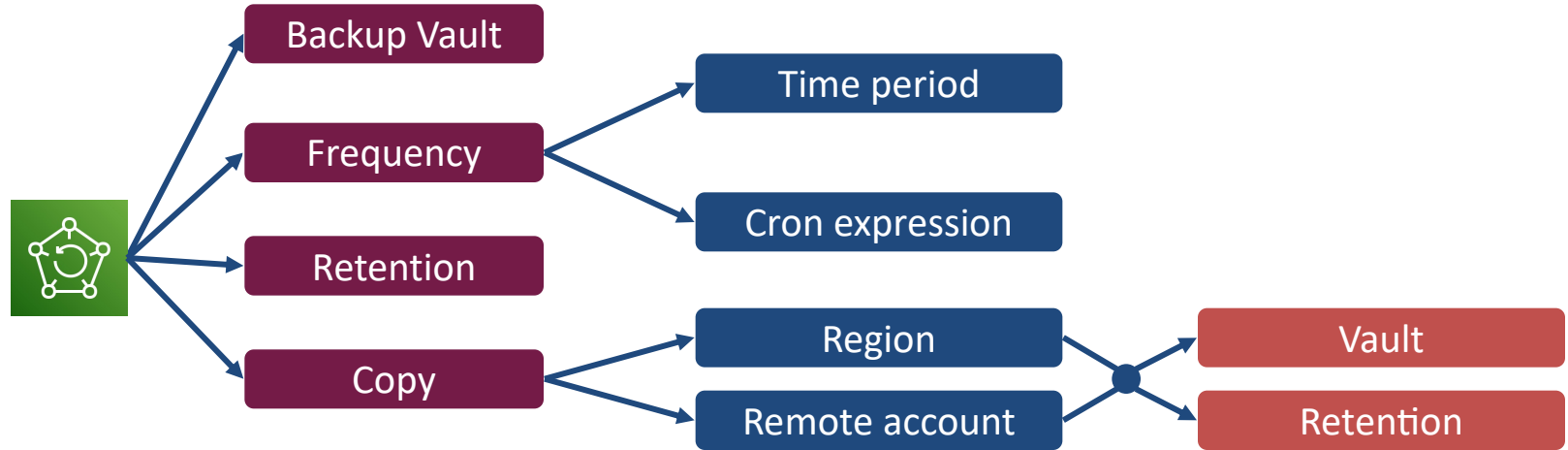
AWS Backup Workflow



AWS Backup Plan Creation



Backup Rule Creation



DEMO

Implement a Backup plan
Initiate an on-demand backup



Implementing Event-based Monitoring

String Metric Filter Basics

Match everything

" "

Single term

"ERROR"

Include/exclude terms

"ERROR" - "permissions"

Multiple terms using AND

"ERROR memory exception"

Multiple terms using OR

?ERROR ?WARN

Space-Delimited Metric Filter Basics

Specify all fields with a name, bounded by [] and separated by commas

Specify unknown number of fields with "..."

Add conditions =, !=, <, <=, >, >=

Utilize * to match partial strings or numbers

Implement AND with &&, OR with |

Space-Delimited Metric Filter Examples

```
[ip, id, user, timestamp, request, status_code = 4*, size]
```

Match all 4XX response codes

```
[ip, id, user, timestamp, request, status_code, size > 1000]
```

Match response sizes >1000 bytes

```
[ip, id, user, timestamp, request, status_code != 3*, size]
```

Ignore all redirect response codes

JSON Metric Filter Basics

{SELECTOR EQUALITY_OPERATOR STRING}

Equality

EQUALITY_OPERATOR is = or !=

Equality

{SELECTOR NUMERIC_OPERATOR NUMBER}

Numeric

NUMERIC_OPERATOR can be =, !=, <, >, <= or >=

Numeric

SELECTOR starts with \$, indicating the root of JSON

Both

SELECTOR supports arrays

Both

Implement AND with &&, OR with ||

Both

Publish numerical value using "metricValue:"

Both

JSON Metric Filter Examples (CloudTrail)

```
{ ($.eventName = ConsoleLogin) && ($.responseElements.ConsoleLogin = "Failure") }
```

Match all console login failures

```
{ ($.eventName = ConsoleLogin) && ($.userIdentity.userName = "csmith") }
```

Match all console logins by IAM user csmith

```
{ $.userIdentity.type = "Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent" }
```

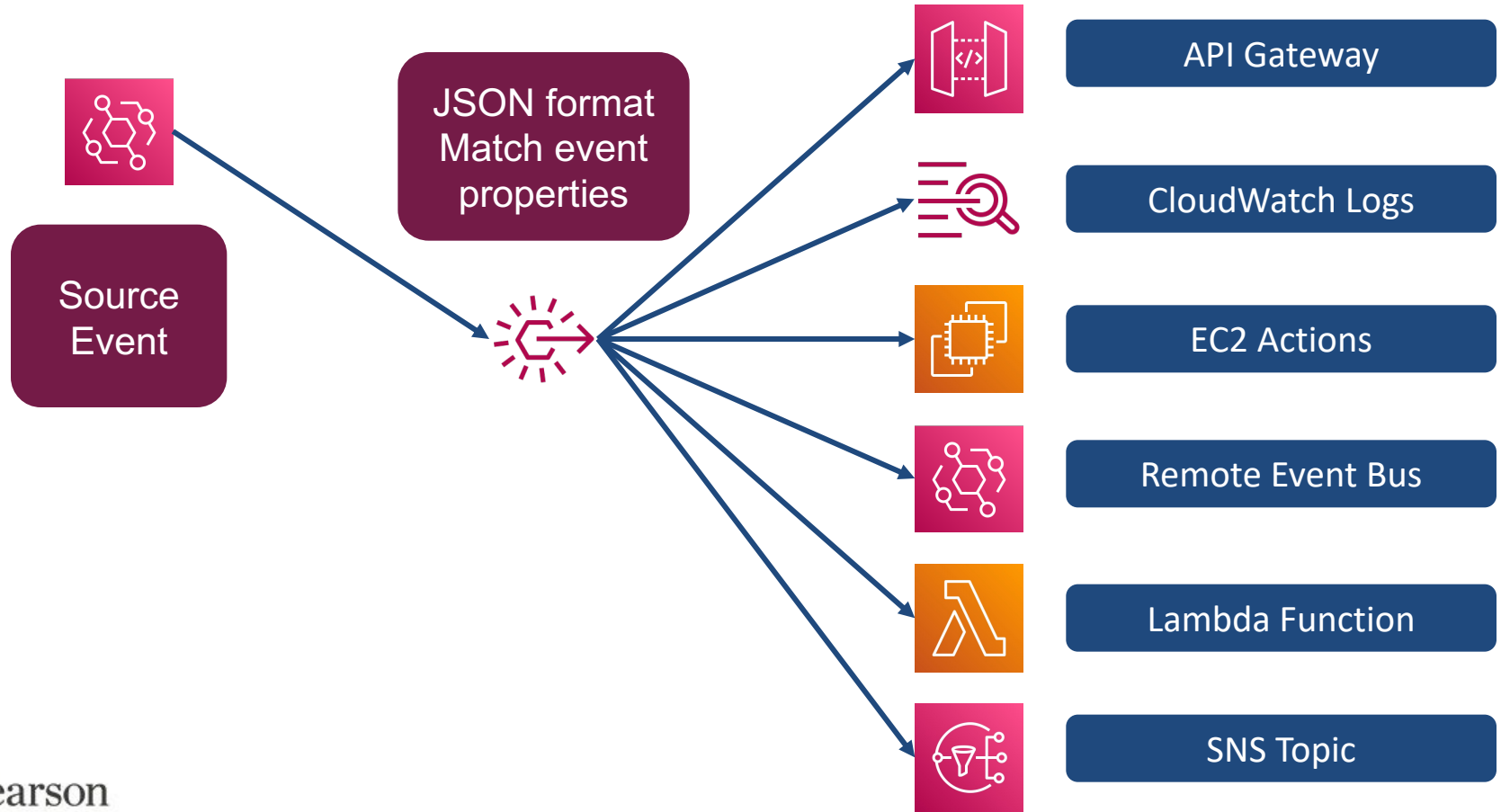
Match all root user activity

EventBridge Basics

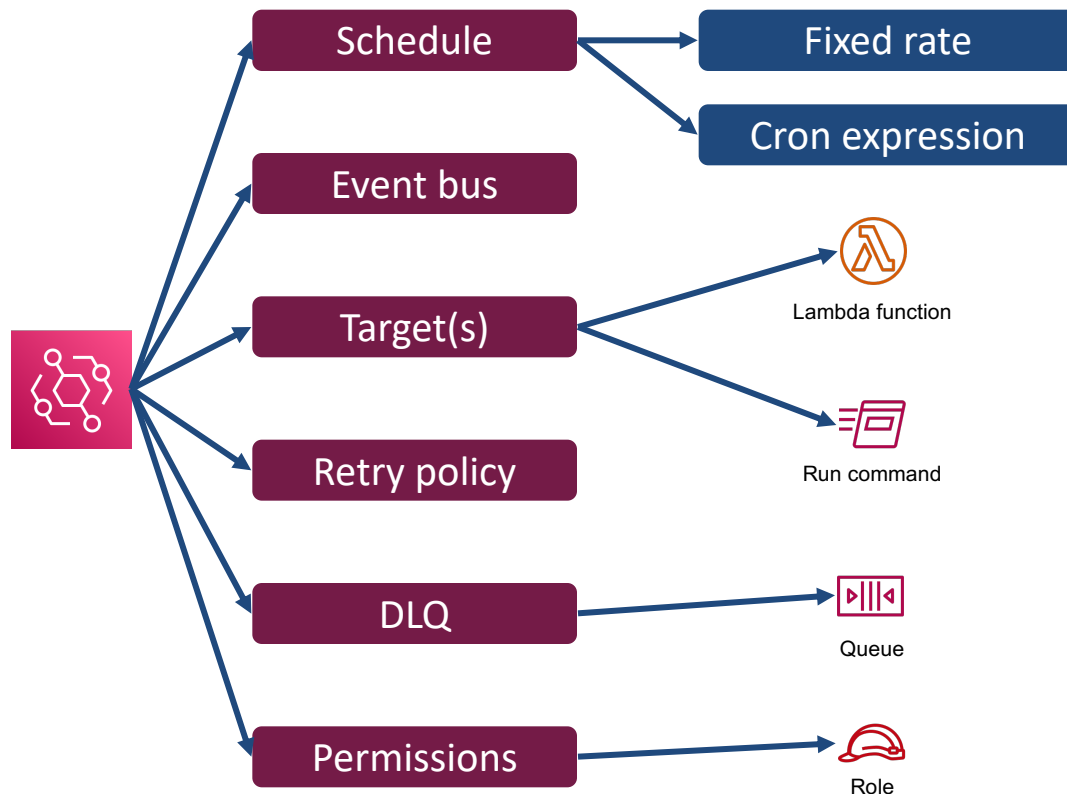


Region scope
Default Event bus
Custom Event bus
Sources and targets
Replay feature
DLQ feature

EventBridge Rules

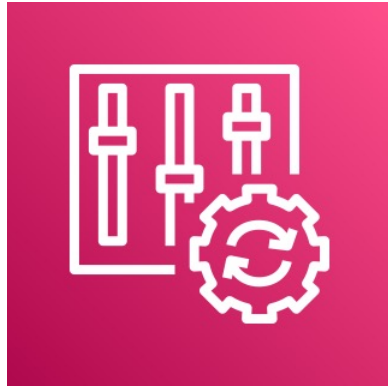


EventBridge Scheduled Rules



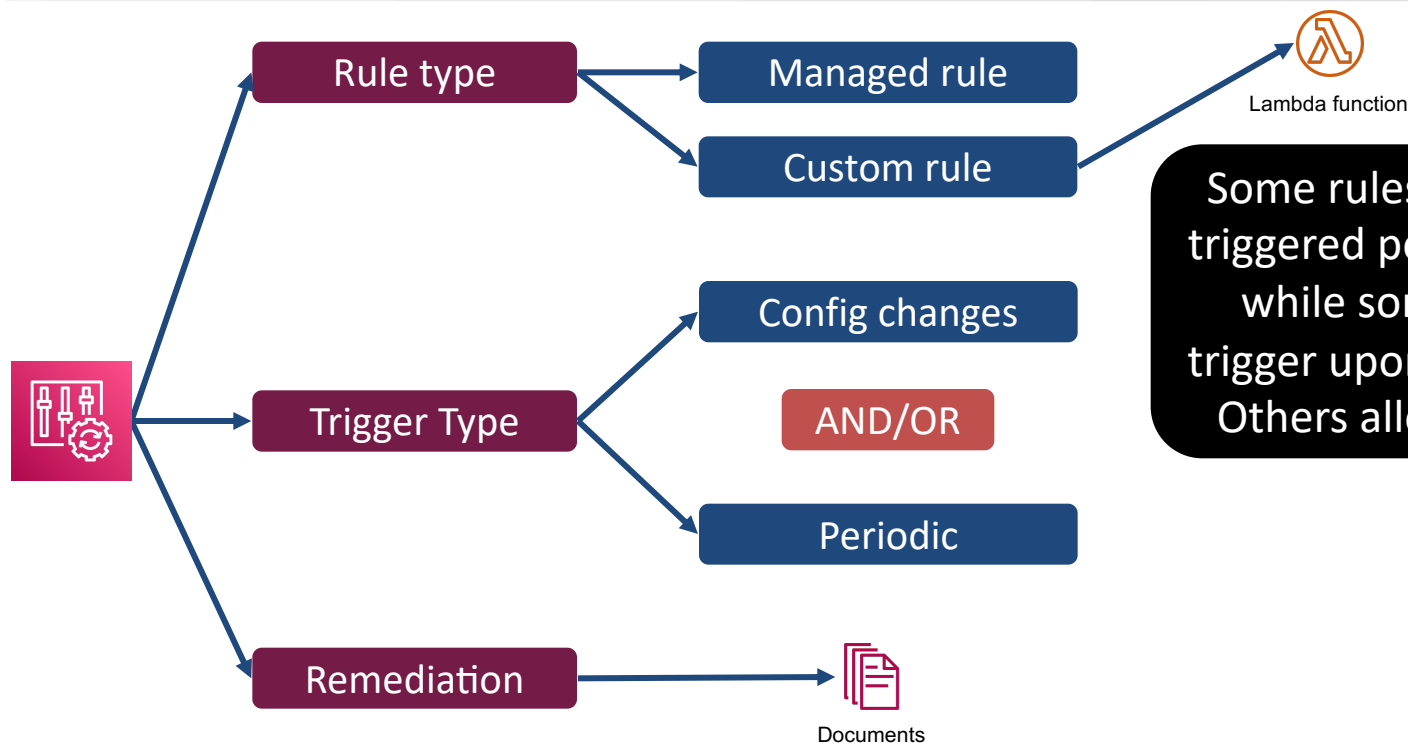
Many of these parameters have default values

Config Basics



Region scope
Config Streams
Partial coverage
Capture changes
Capture config
Snapshots

Config Rules



Some rules must be triggered periodically, while some only trigger upon changes. Others allow both!

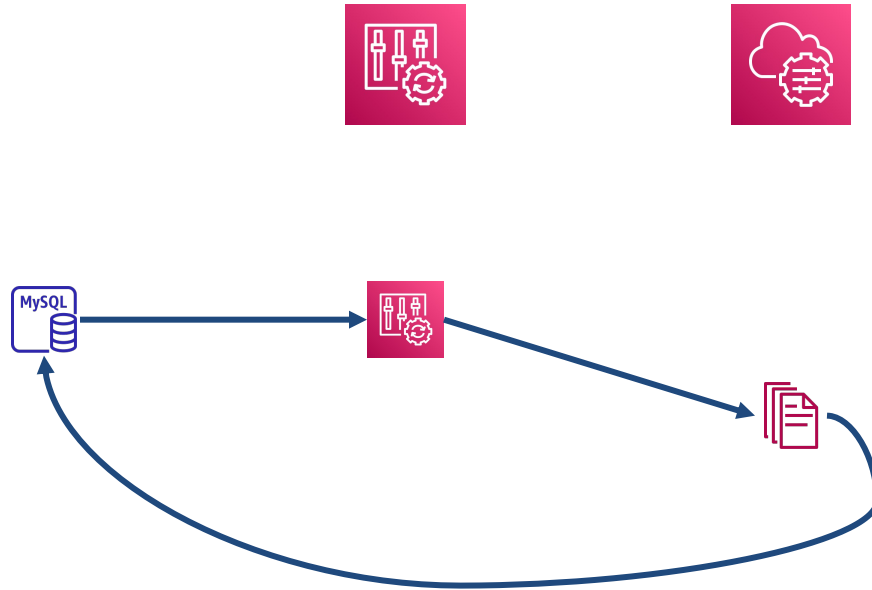
Config Rule Remediation Example

Config stream



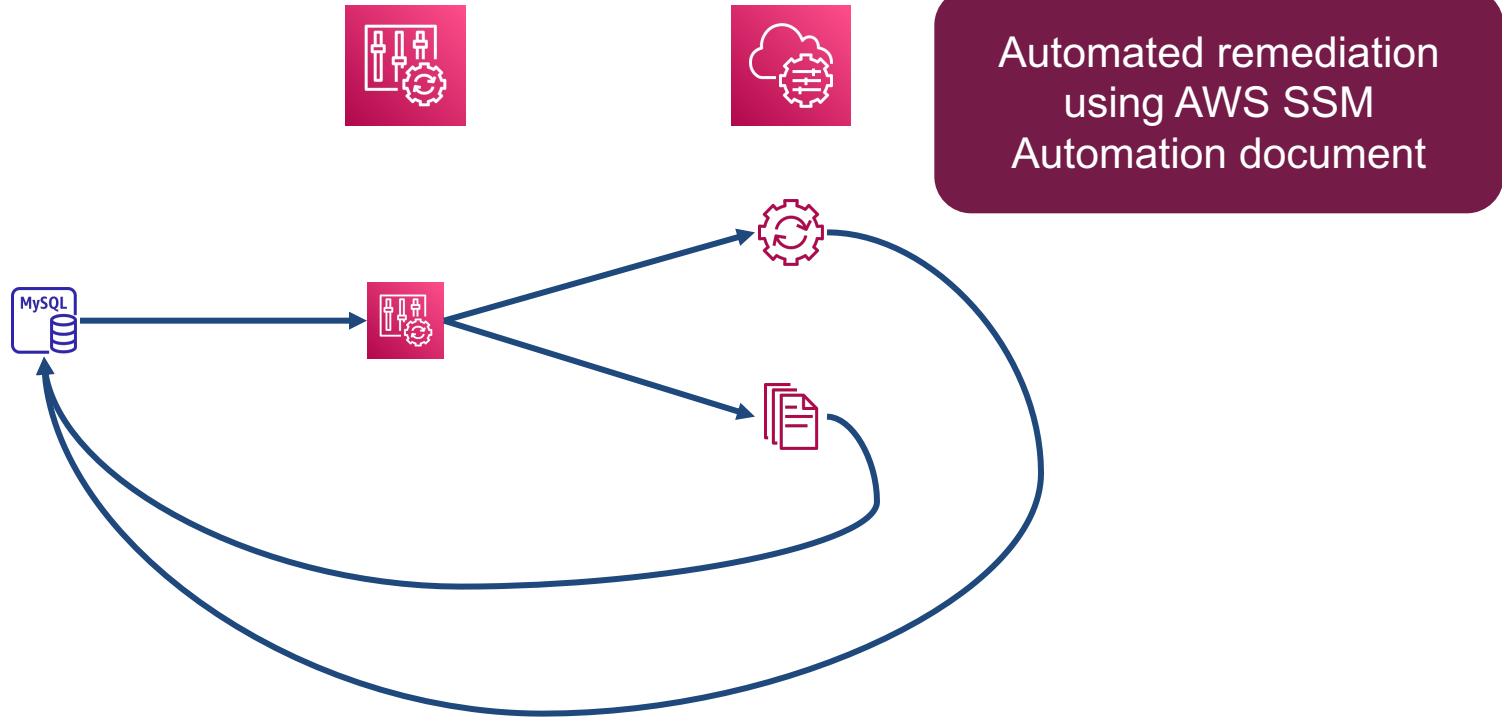
RDS instance with
Enhanced Monitoring
disabled

Config Rule Remediation Example



Manual remediation using
AWS SSM document

Config Rule Remediation Example



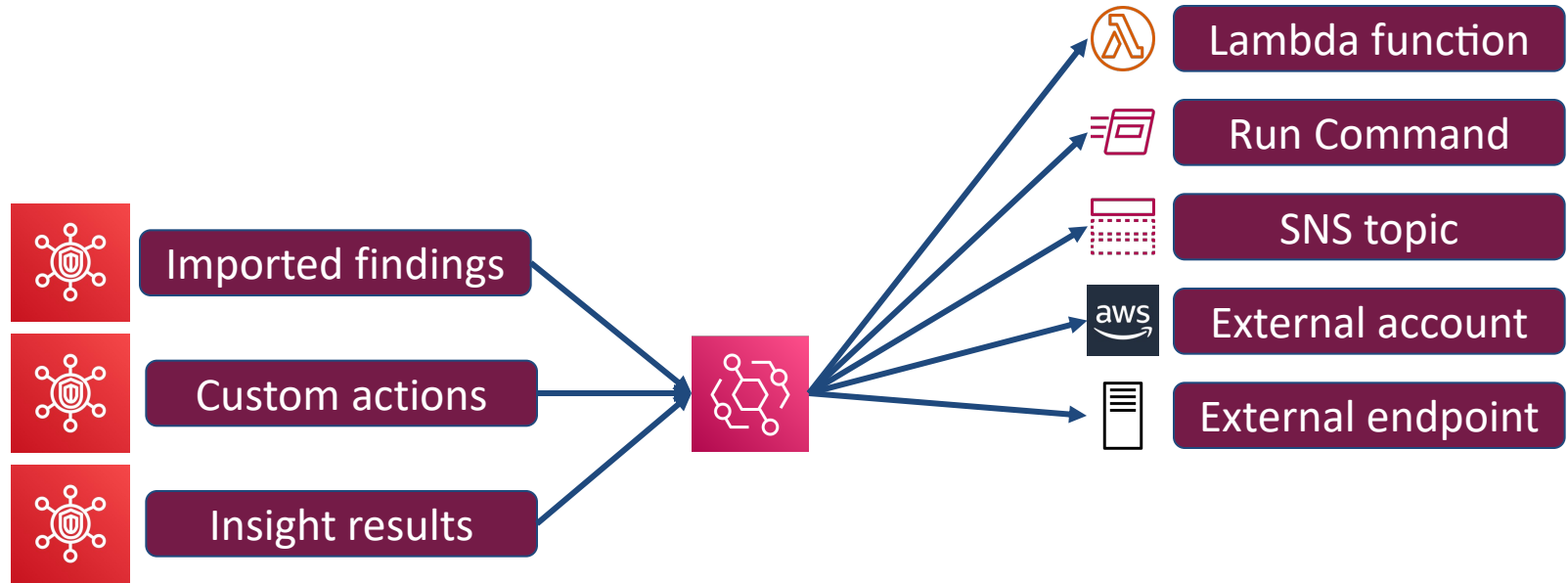
DEMO

Create monitoring workflow notifying via SNS for any termination of EC2 instances

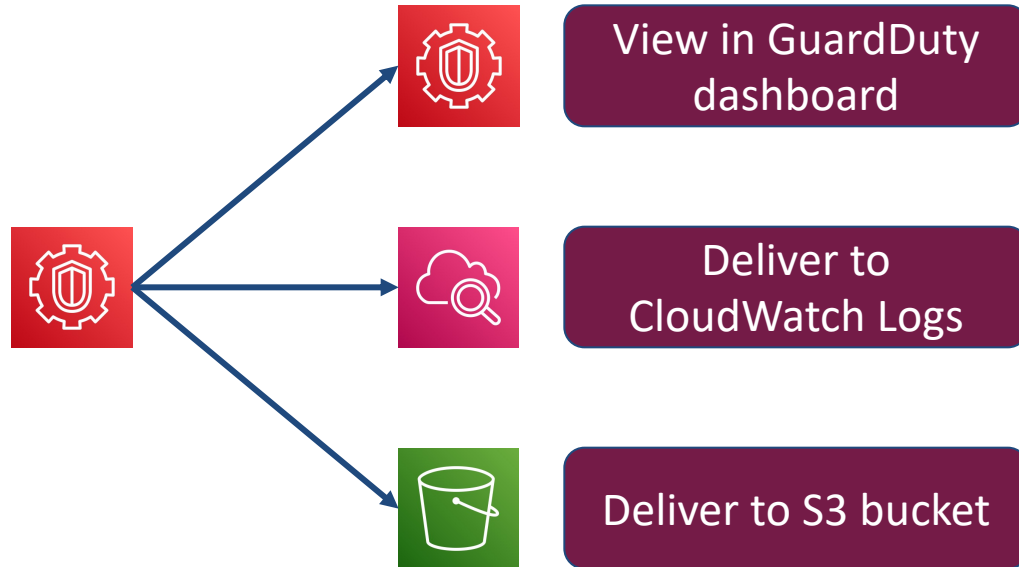


Security Vulnerability Mitigation

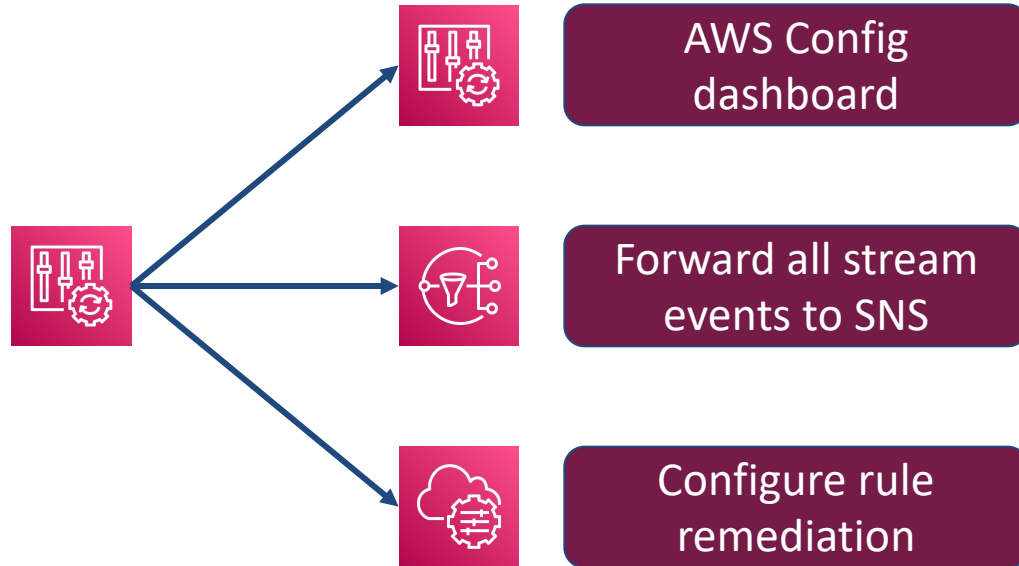
Remediation Workflow



GuardDuty Findings Review



AWS Config Review



Inspector Main Use Cases



Facilitate golden AMI
Audit existing instances
On-demand rule
evaluation

Inspector Resource Creation

Prerequisites

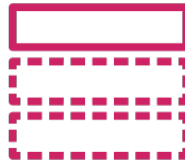


Inspector Agent
Installed on EC2

Which can be
installed
automatically.....if:



Systems Manager
Agent Installed



You also need an
SNS topic

Inspector Resource Creation

Parameters

Assessment
Template

Which
contains 1
or more of
the
following:

1. Network Reachability
2. Security Best Practices
3. CVE
4. CIS OS Sec Benchmark
5. Runtime Behavior Analysis

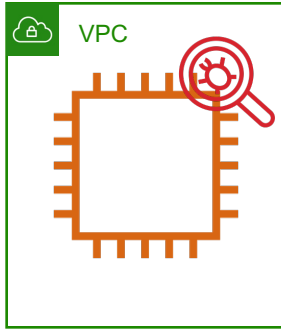
and...

EC2
assessment
target(s)

Optional

Required

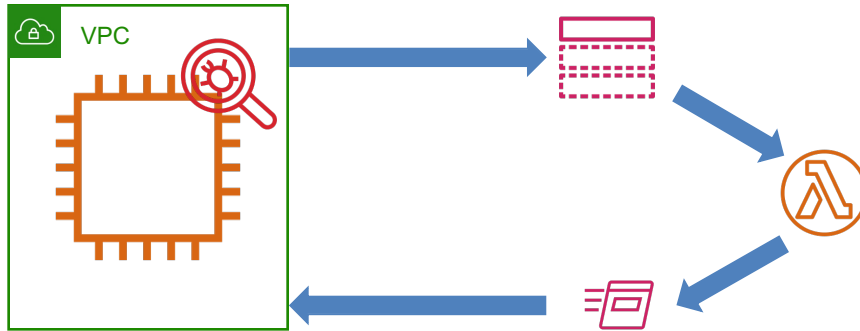
Host-based Security



- Install Inspector Agent
- Create SNS topic
- Configure assessment template
- Schedule assessment runs
- Execute assessment

Use Amazon Inspector

Host-based Security



- Finding posted to SNS
- Lambda parses finding
- Lambda invokes SSM Run Command
- Run Command installs patch on EC2 instance

Automatically remediate findings

DEMO

Install Inspector Agent on EC2
Implement Inspector Assessment Run



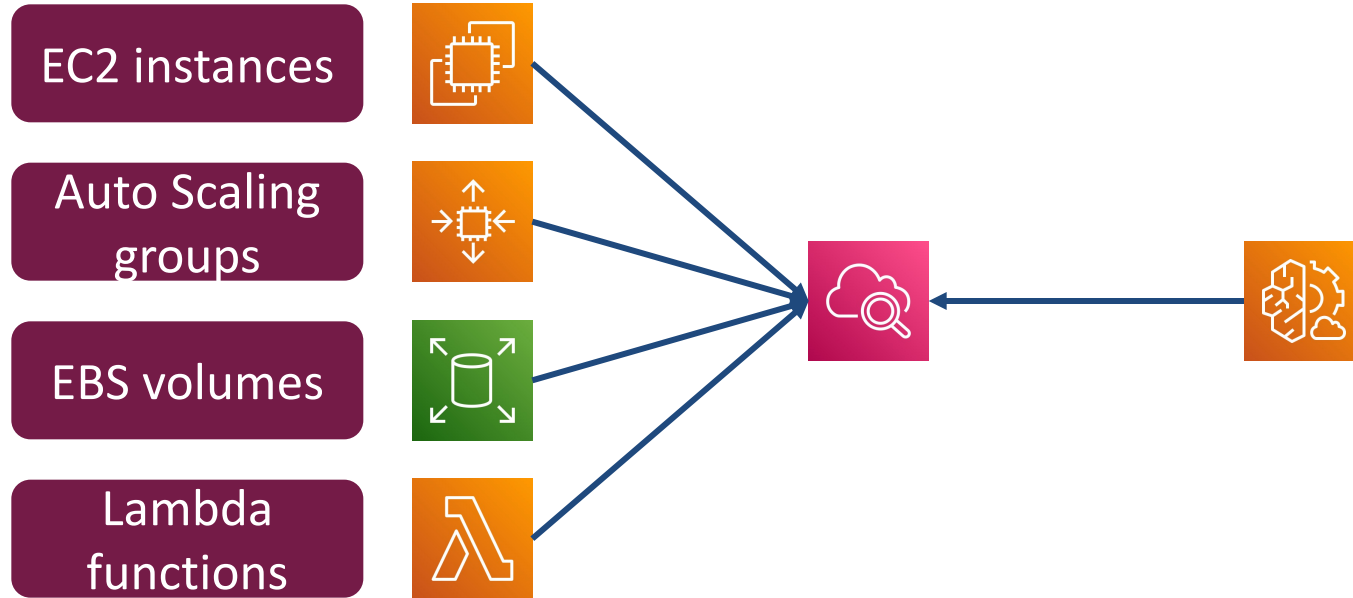
Cost Optimization

AWS Compute Optimizer Basics

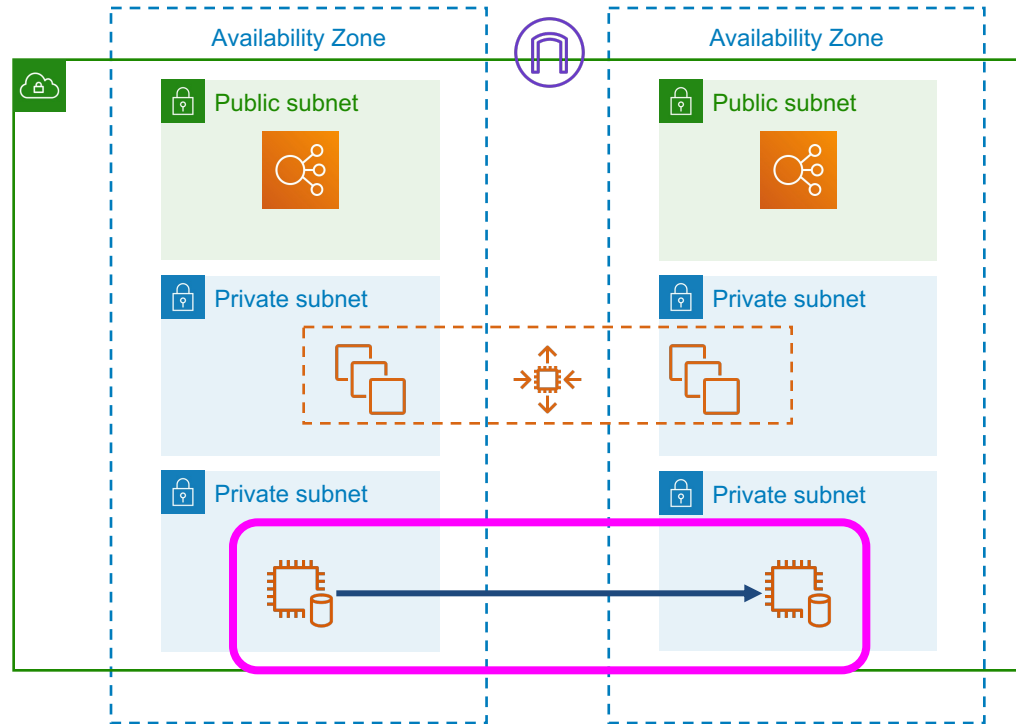


Analyze compute resources
Analyze single account
Analyze entire organization
30 hours metrics minimum
Recommends optimization

AWS Compute Optimizer Services



Relational Database Workloads



You can implement the DB on EC2 instances, including....

Backups

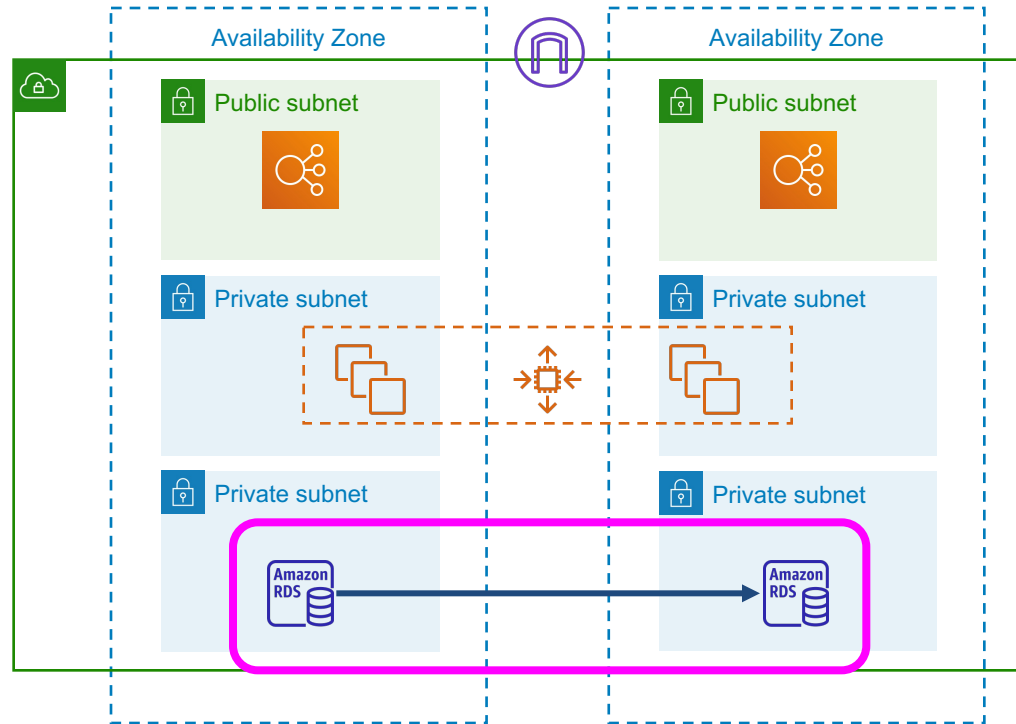
Replication

Software updates

Failover

Restores

Relational Database Workloads



OR, you can deploy RDS and delegate all of these operations to the service

Backups

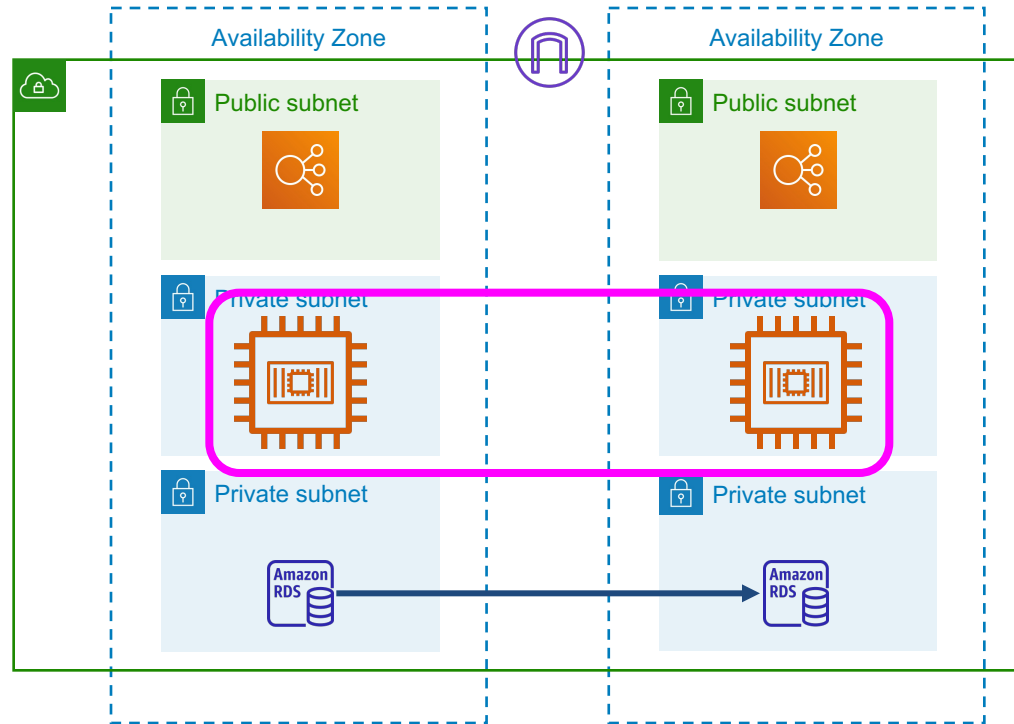
Replication

Software updates

Failover

Restores

Container Workloads



You can implement Docker containers on EC2 instances, including....

Deployment

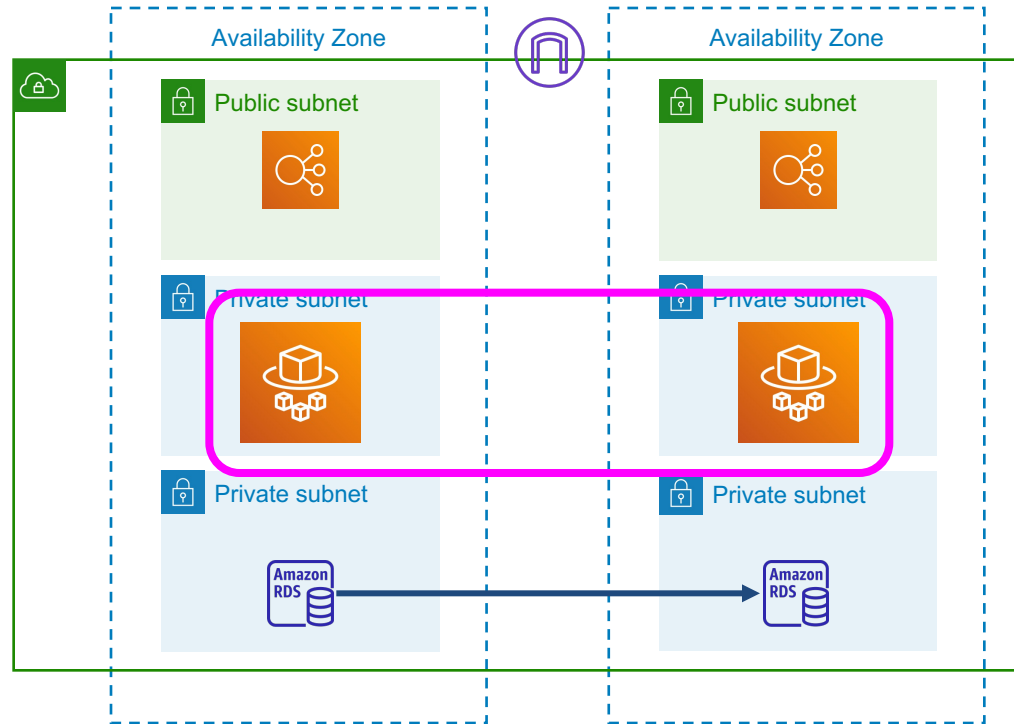
Container scaling

EC2 scaling

OS updates

Rollbacks

Container Workloads



OR, you can deploy using Fargate and delegate these operations to the service

Deployment

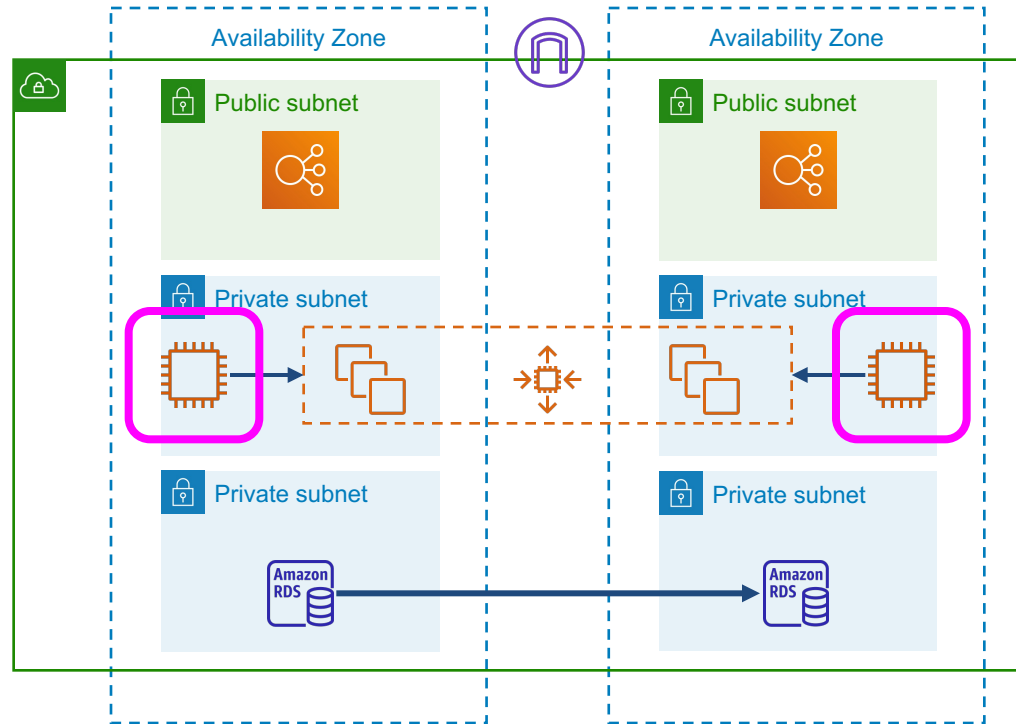
Container scaling

EC2 scaling

OS updates

Rollbacks

Shared Filesystem Workloads



You can implement a shared filesystem on EC2, including....

Backups

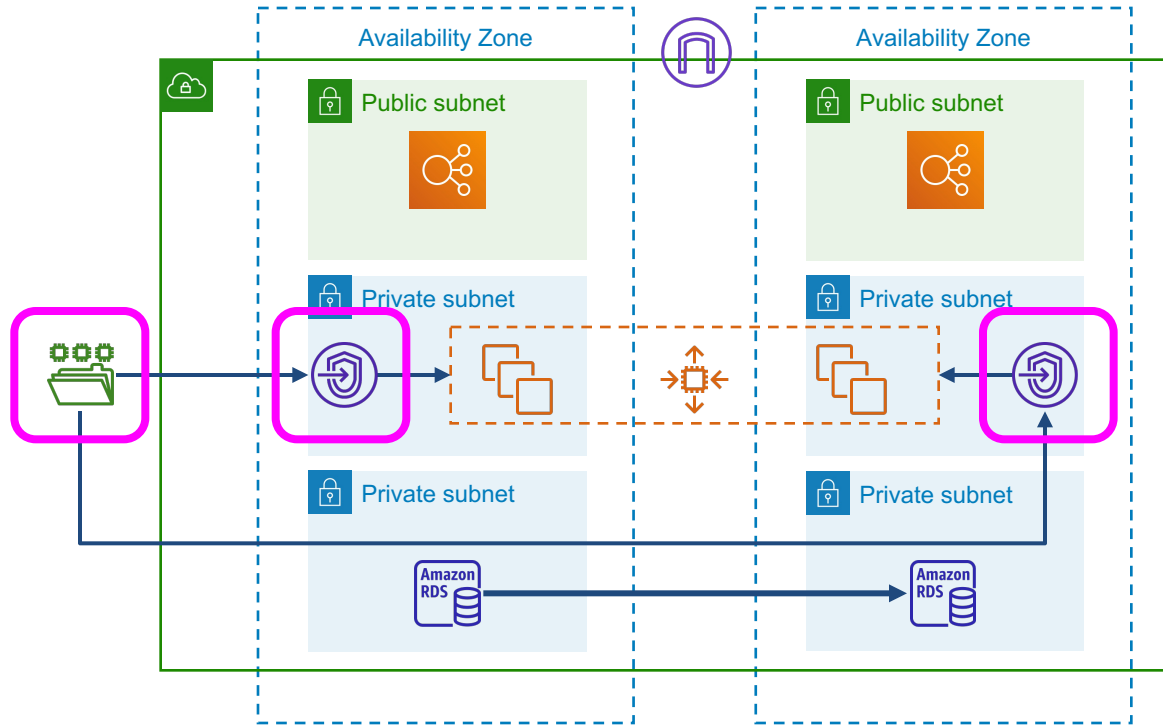
Replication

Software updates

Failover

Restores

Shared Filesystem Workloads



Or you can deploy a single EFS file system with mount points in each AZ

Backups

Replication

Software updates

Failover

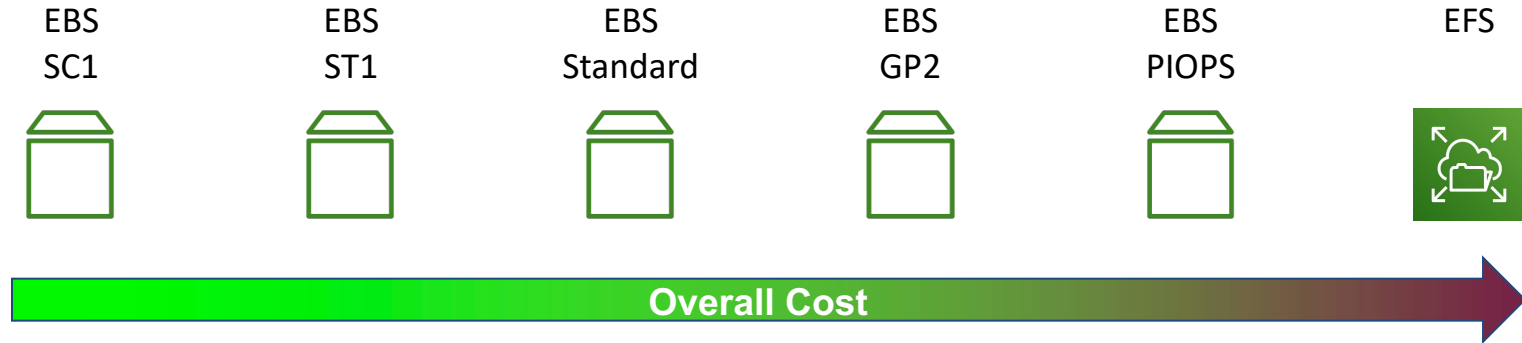
Restores

Compute Cost - EC2 Pricing

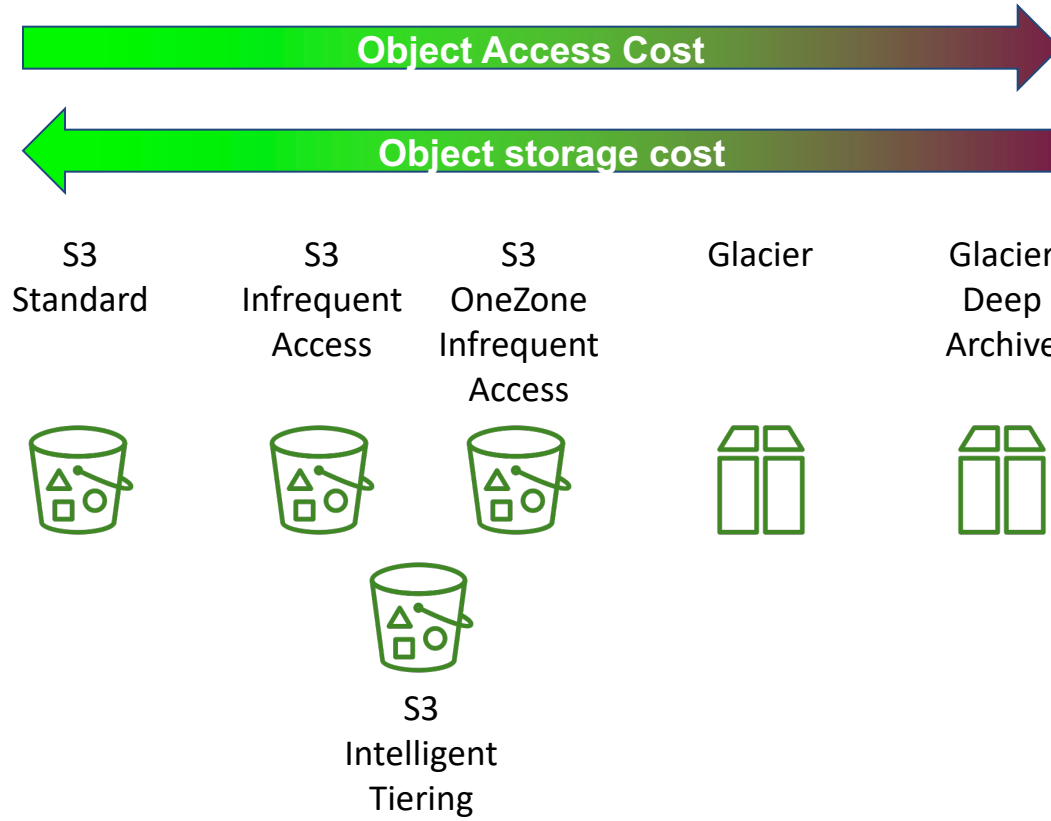
Spot Instances	RI/SPs	On Demand Instances	Dedicated Instances	Dedicated Hosts
<ul style="list-style-type: none">No guaranteed pricingPay for unused capacityVolatileSpecify maximum bid+Specific duration+Multiple instance types+Multiple AZ	<ul style="list-style-type: none">Guaranteed pricing for up to 3 years+Capacity guaranteeVariable up-front for more discountSavings Plans for more flexibility	<ul style="list-style-type: none">Pay as you goNo discountNo capacity guarantee	<ul style="list-style-type: none">Dedicated hardwareCan share with non-dedicated VMsPer-region fee+Spot+Reservations+On Demand	<ul style="list-style-type: none">Dedicated hardwareSingle instance typePay for host capacity, not instance+Reservations+On Demand
Overall Cost				

Storage Cost - Block and File

Storage prices drop over time. It is better to understand current
RELATIVE pricing!



Storage Cost - Object



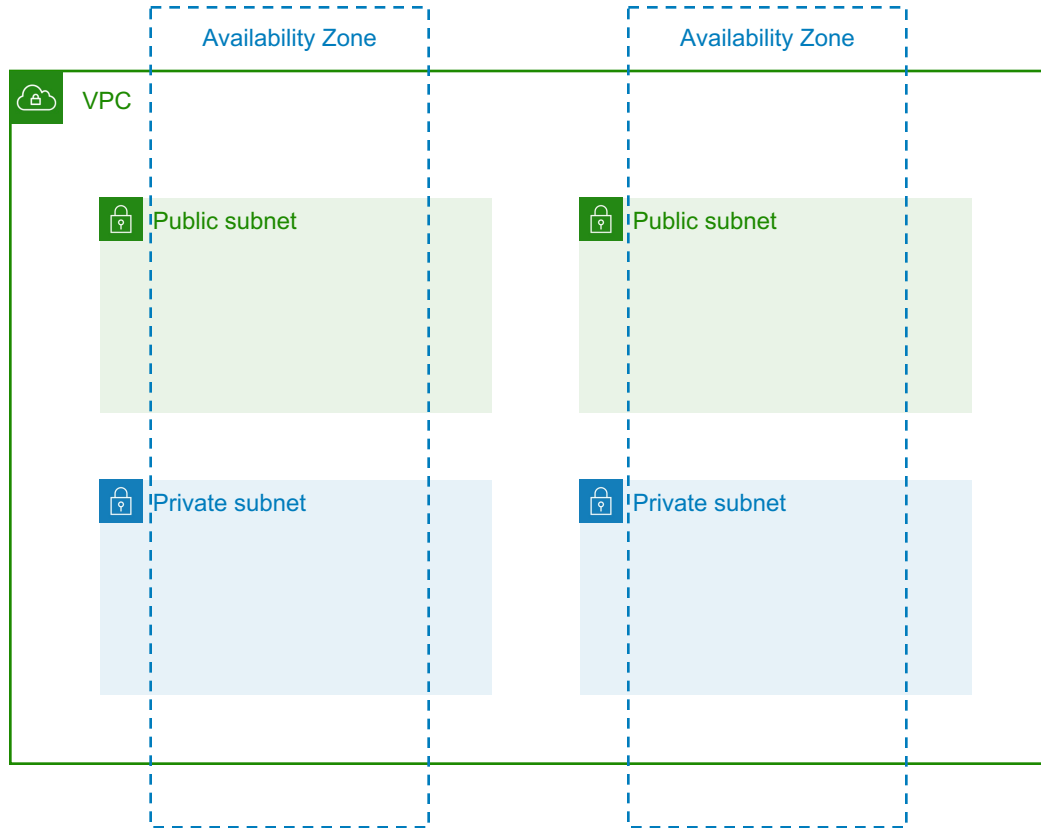
Zero-cost VPC Network Resources



VPC

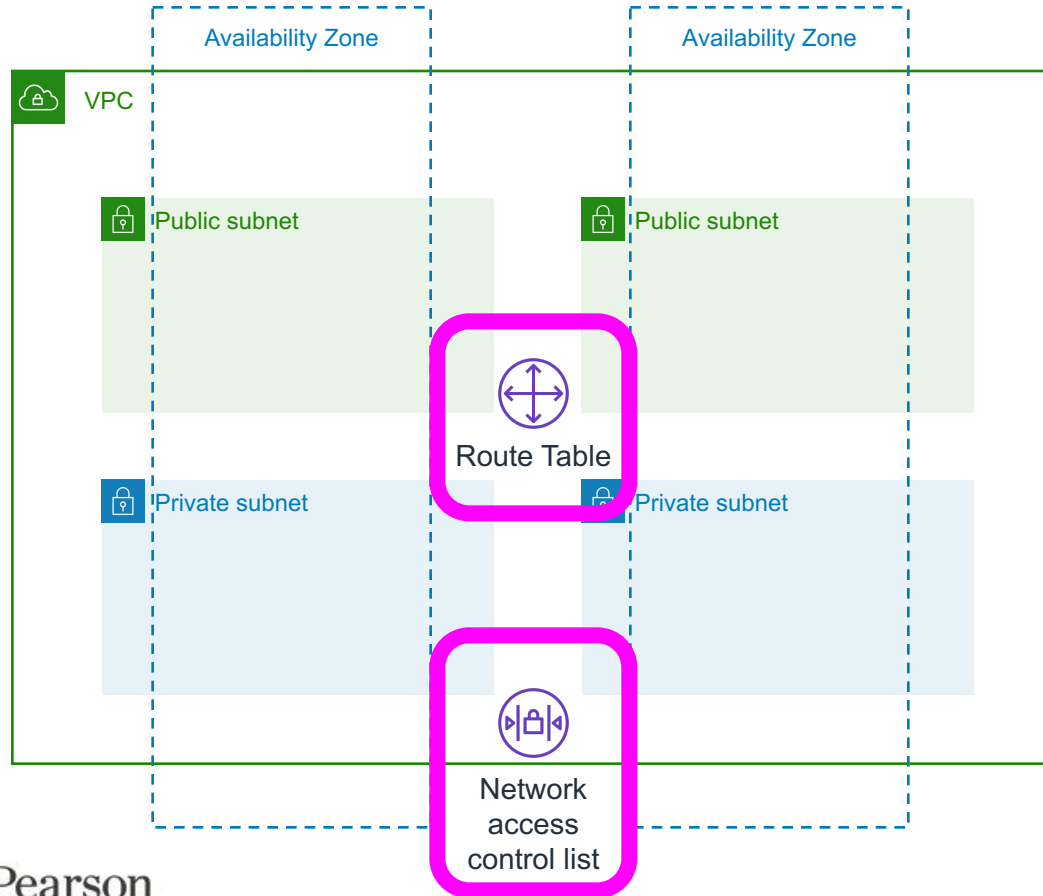
The VPC network may be
free, but it is useless
without other features!

Zero-cost VPC Network Resources



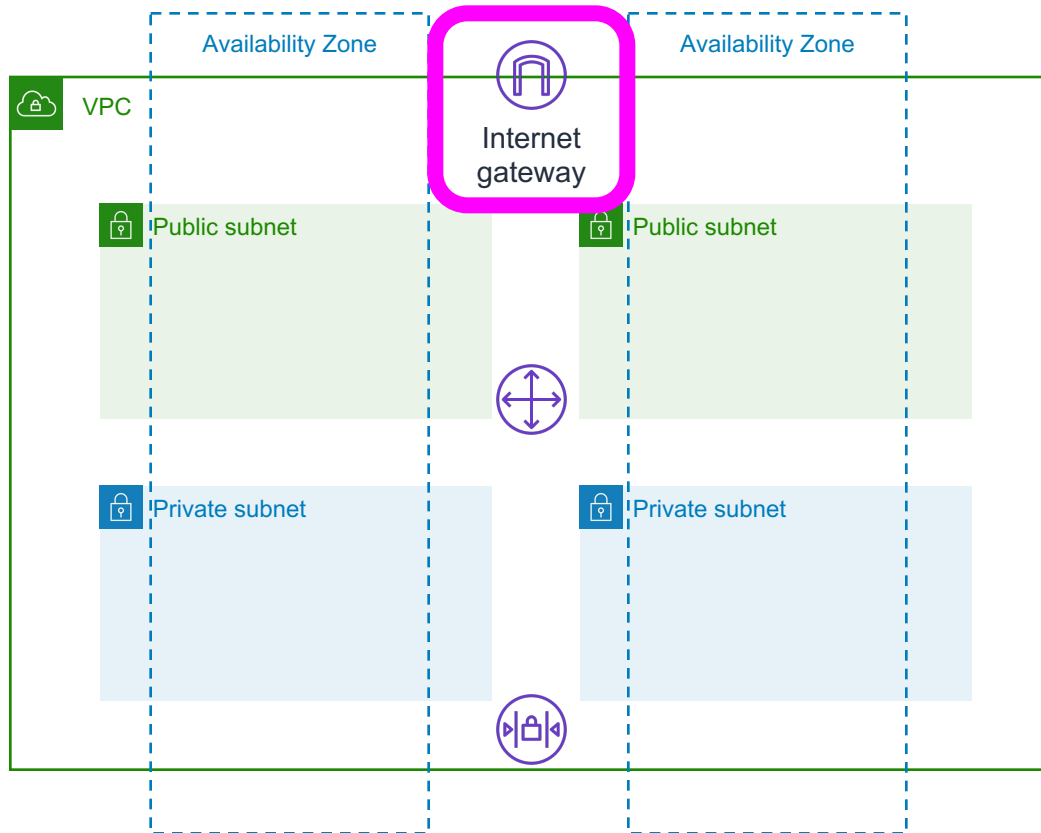
Subnets are free,
regardless of how many
AZ are used in the region

Zero-cost VPC Network Resources



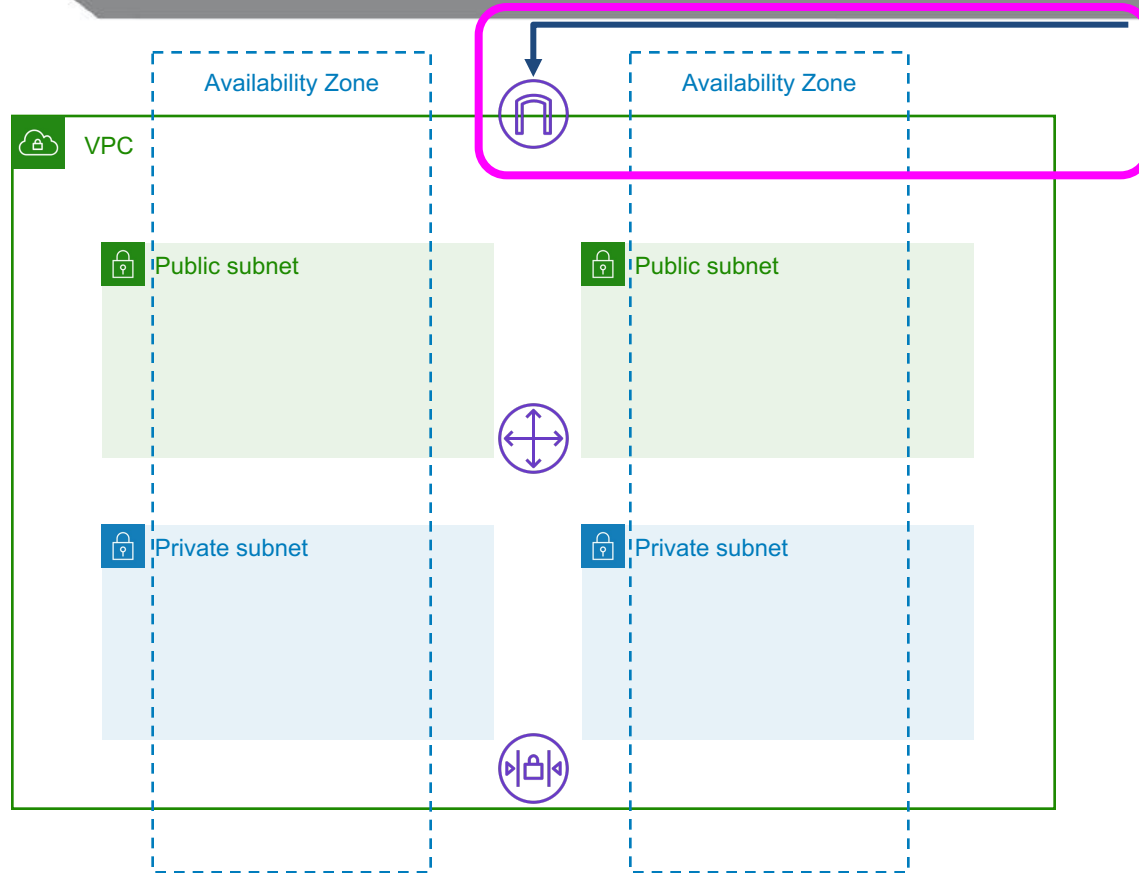
Route tables and NACLs are free, and only limited by account quotas

Zero-cost VPC Network Resources



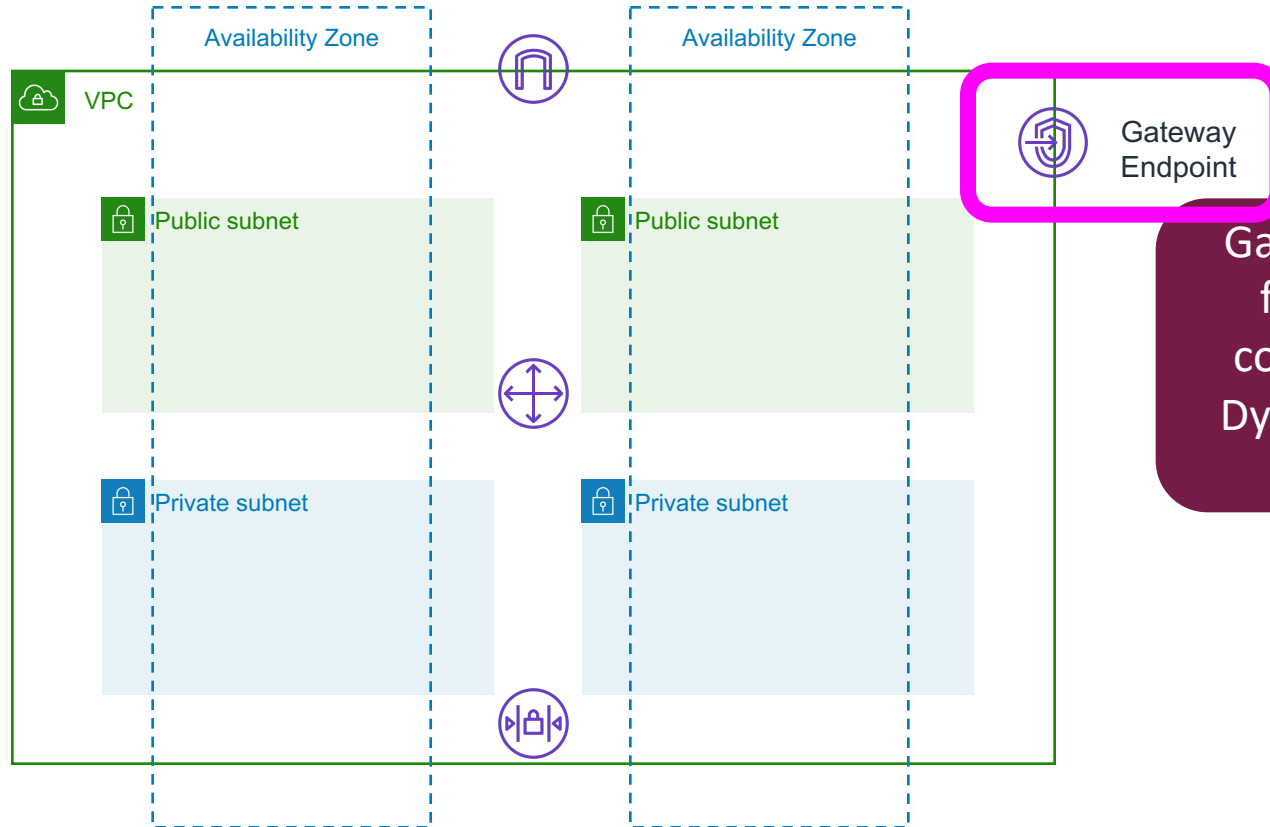
Internet Gateway
resources are free,
regardless of traffic
throughput

Zero-cost VPC Network Resources



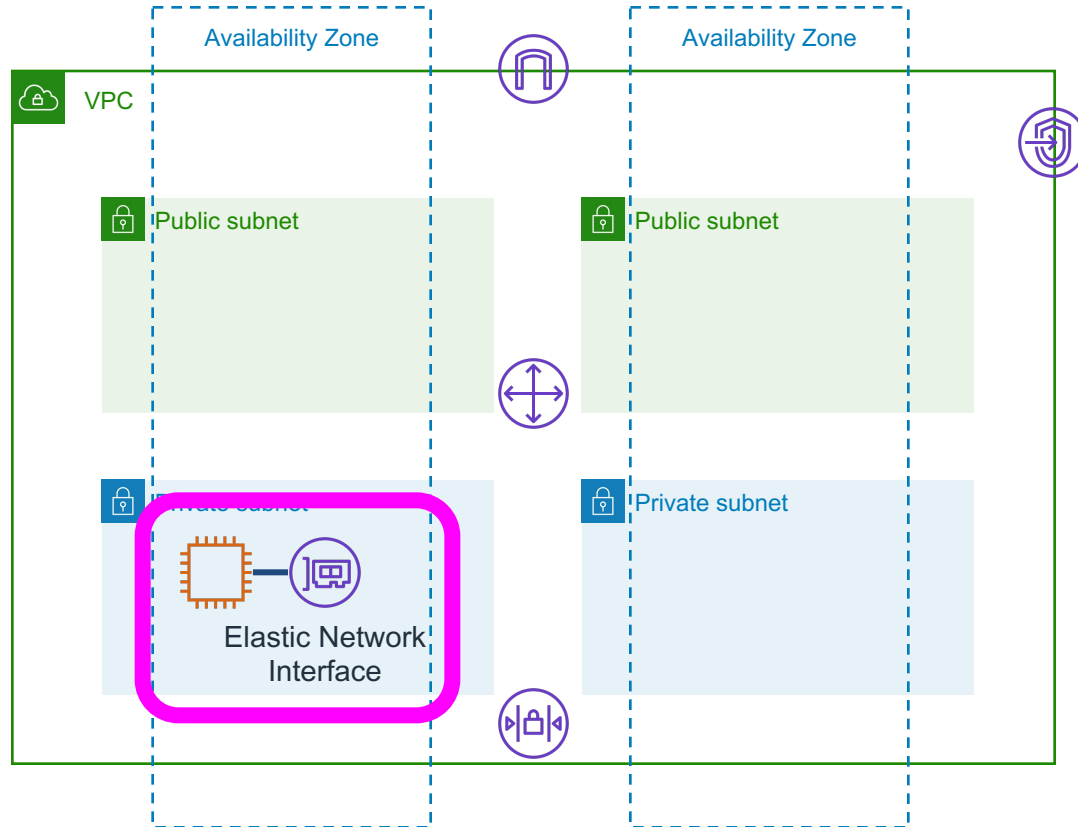
Inbound traffic from the Internet is free, regardless of source

Zero-cost VPC Network Resources



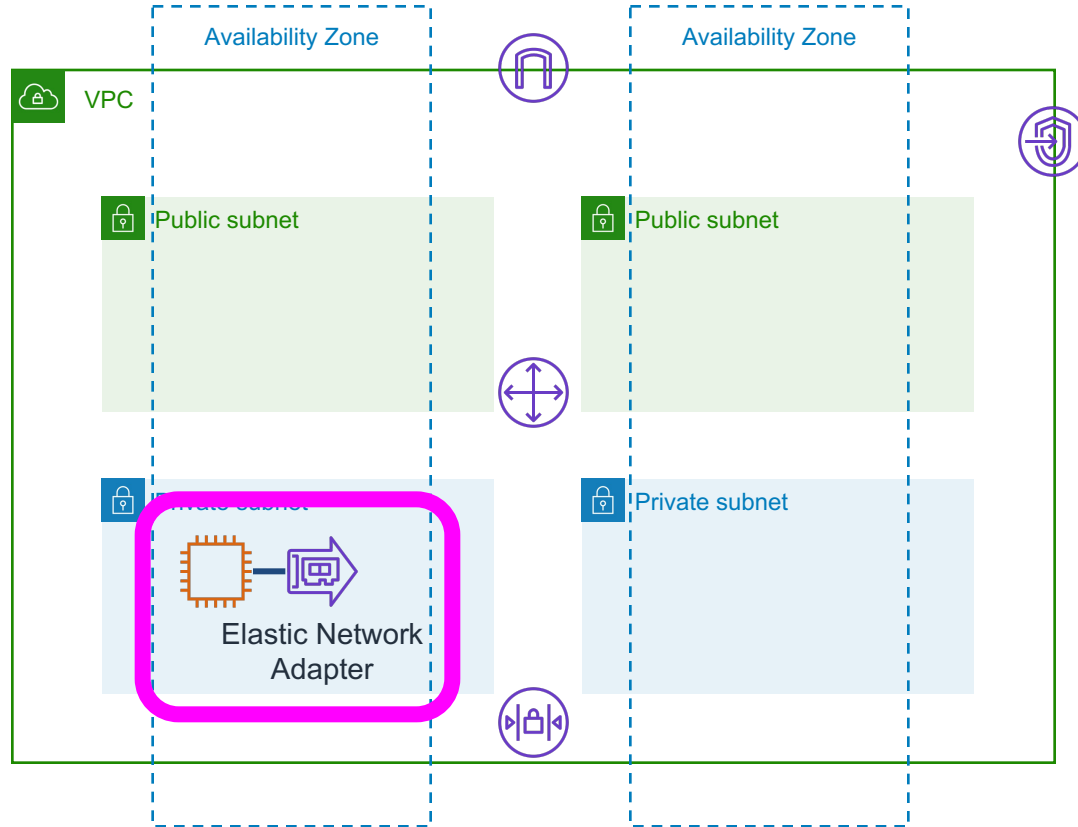
Gateway Endpoints are free, but only allow connectivity to S3 and DynamoDB in the same region

Zero-cost VPC Compute Resources



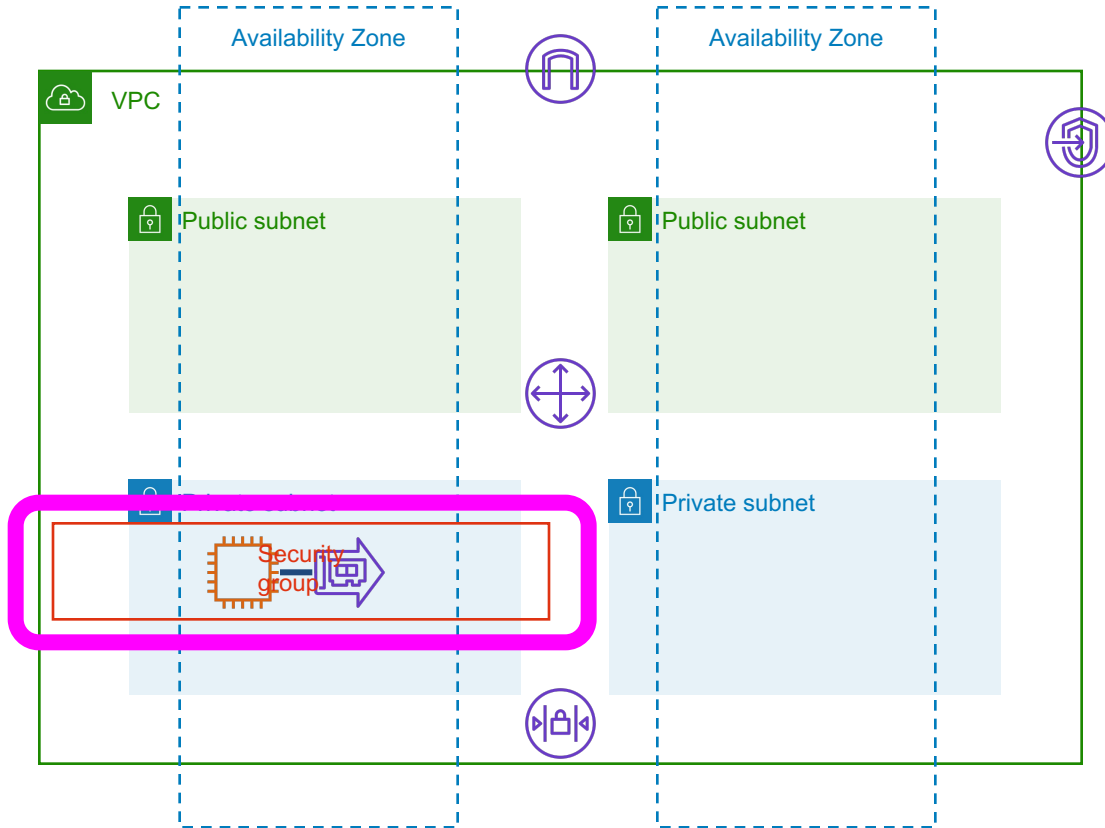
The ENI resource is free, but you may be charged for traffic depending on destination

Zero-cost VPC Compute Resources



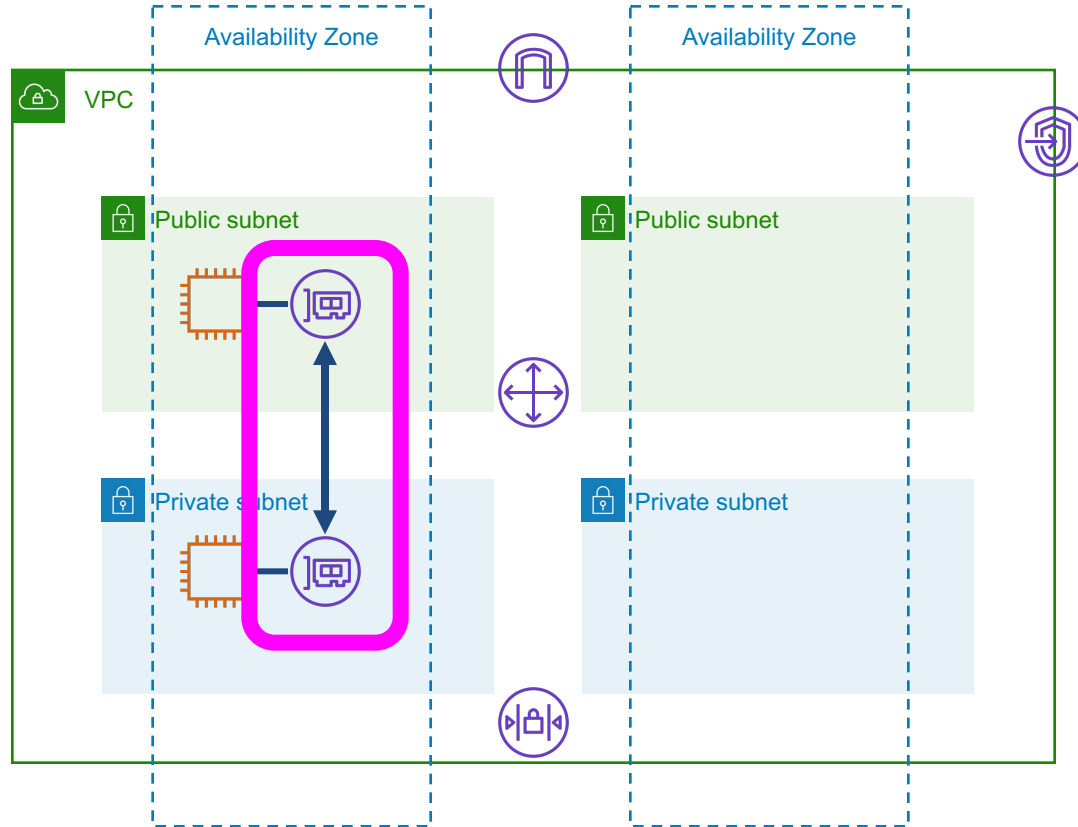
The ENA and Elastic Fabric Adapters are similar to ENI - free but possible charges for network activity

Zero-cost VPC Compute Resources



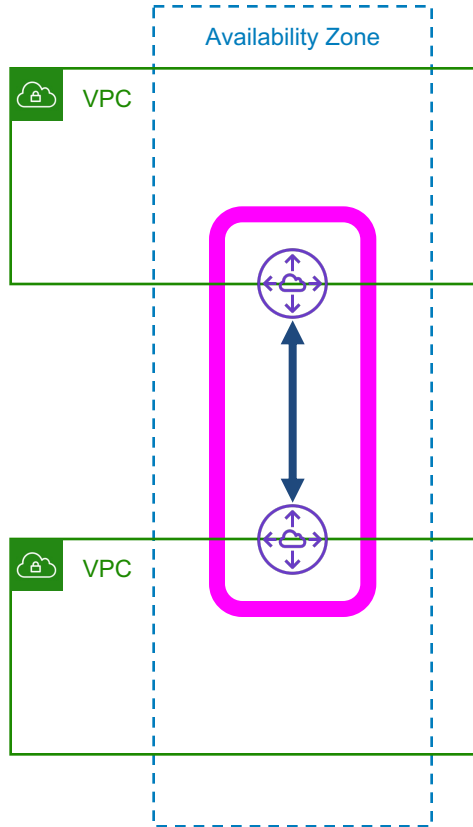
Security groups and rules are free, and only limited by account quotas

Zero-cost VPC Compute Resources



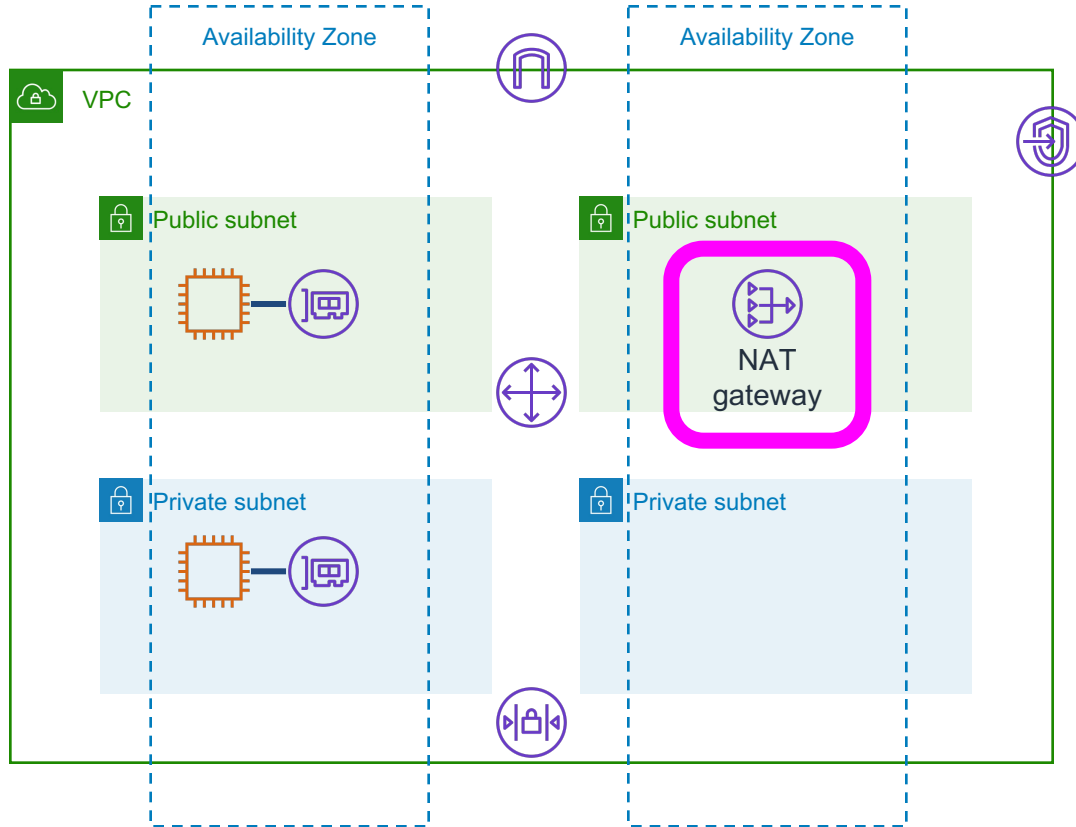
Same-AZ network traffic is free EXCEPT if a public IP is the destination

Zero-cost VPC Compute Resources



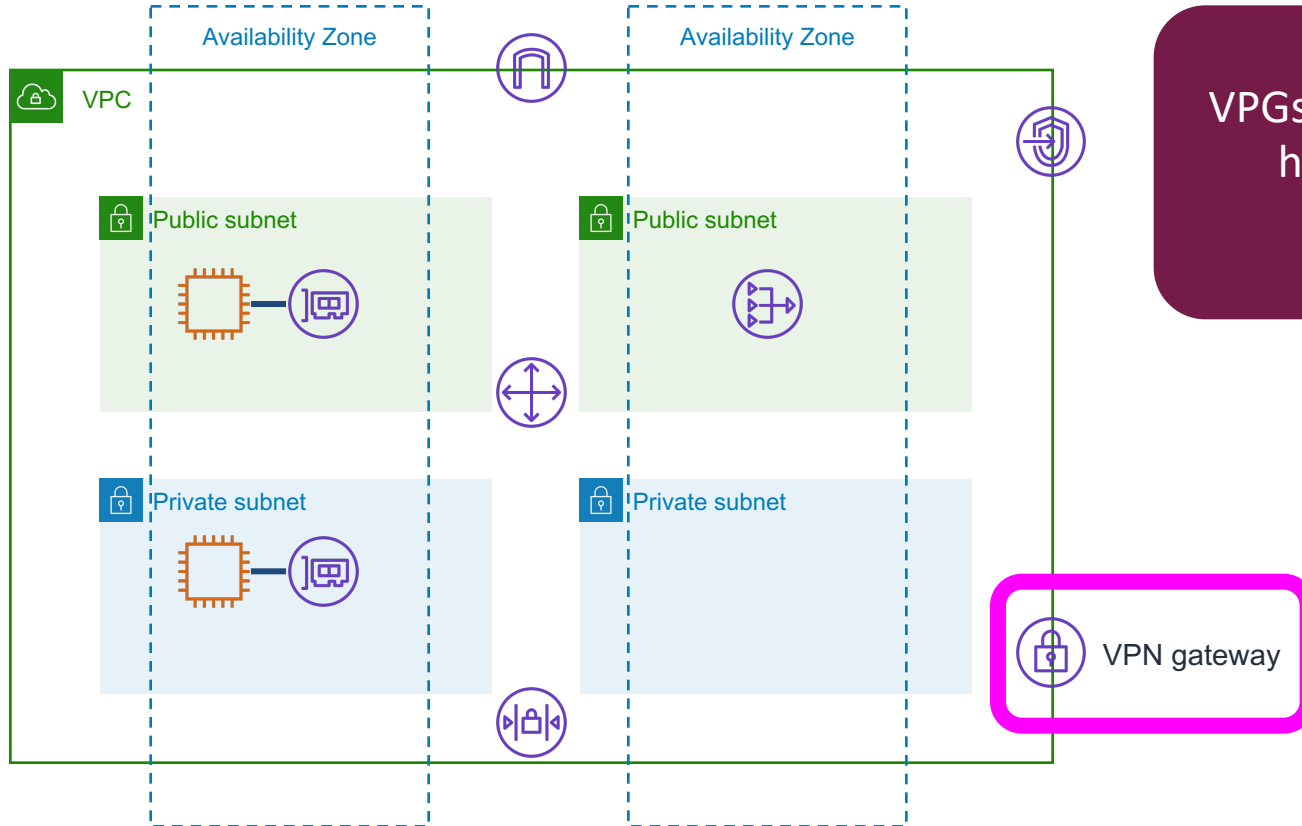
Same-AZ VPC Peering traffic is free, as long as the public IP of the destination is not used

Charged VPC Network Resources



NAT Gateways are charged by the hour and based on throughput

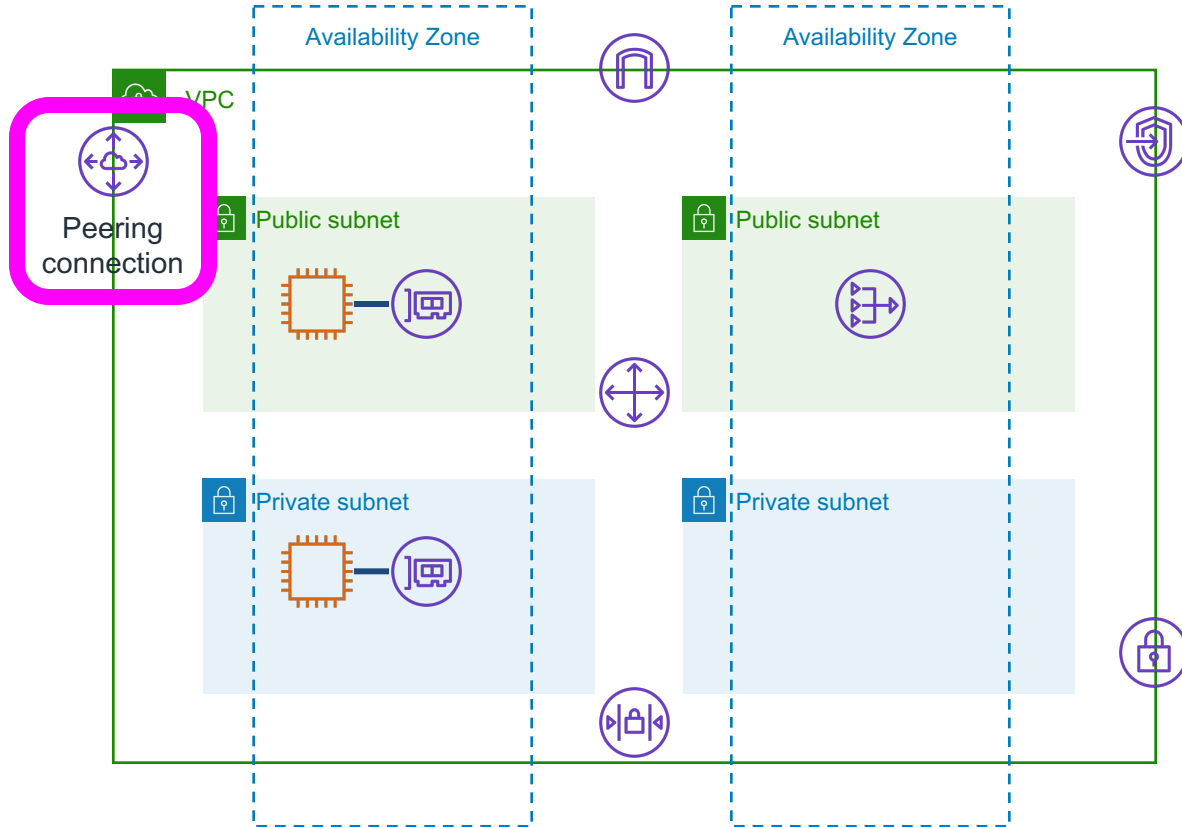
Charged VPC Network Resources



VPGs are charged by the hour and for VPN throughput

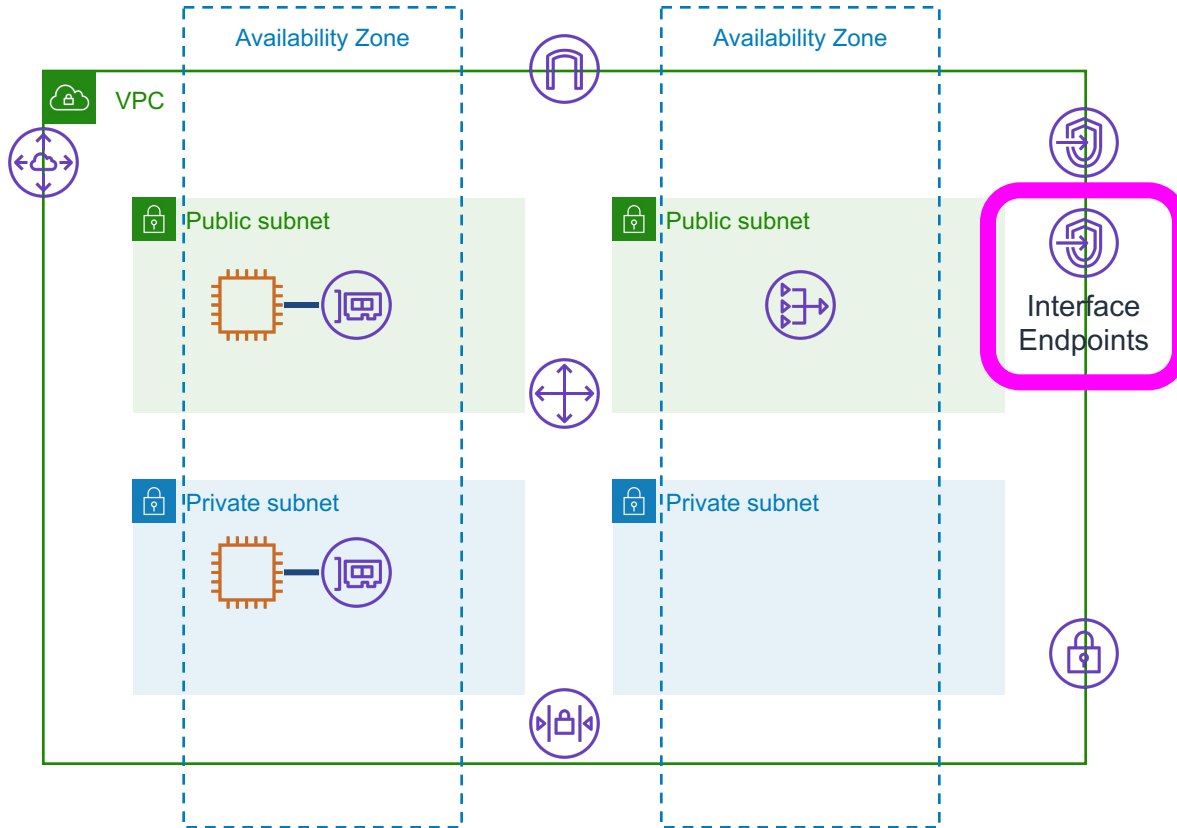
VPN gateway

Charged VPC Network Resources



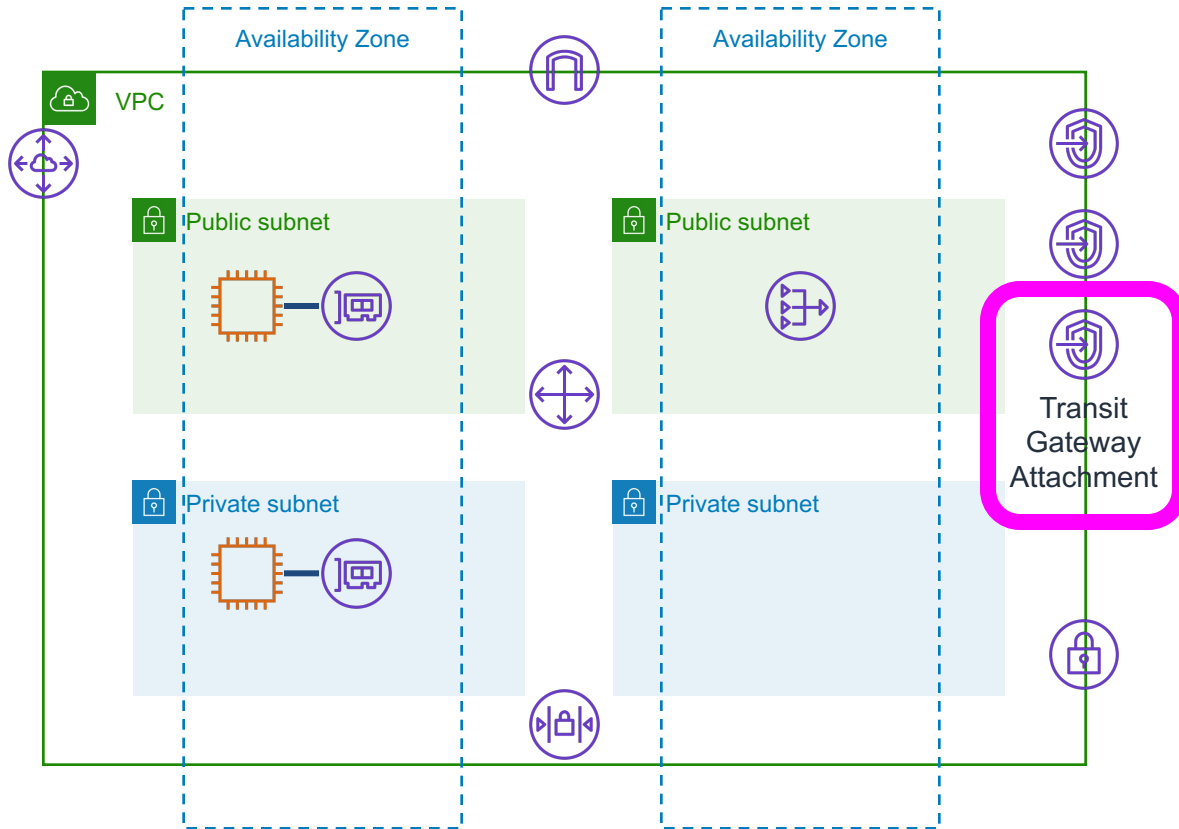
VPC Peering connections are charged by the hour and for traffic throughput, if cross-AZ or cross-region

Charged VPC Network Resources



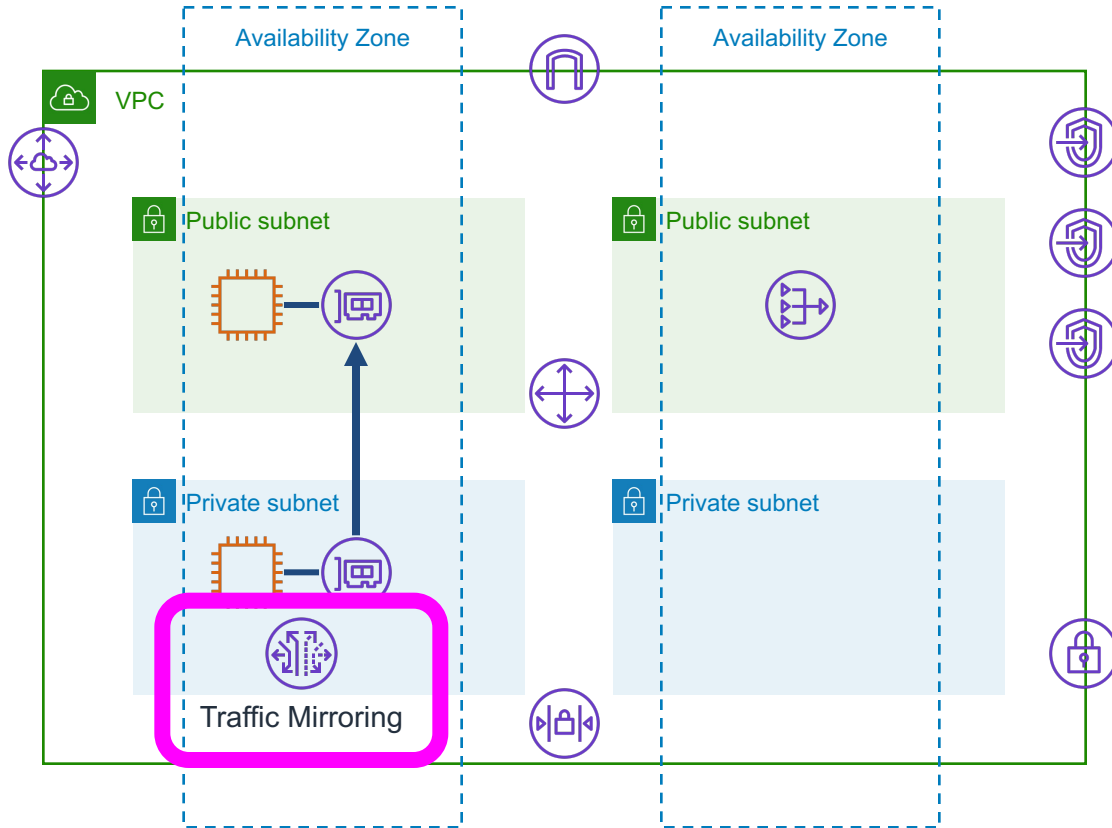
Interface Endpoints and
PrivateLink are charged by
the hour and for traffic
throughput

Charged VPC Network Resources



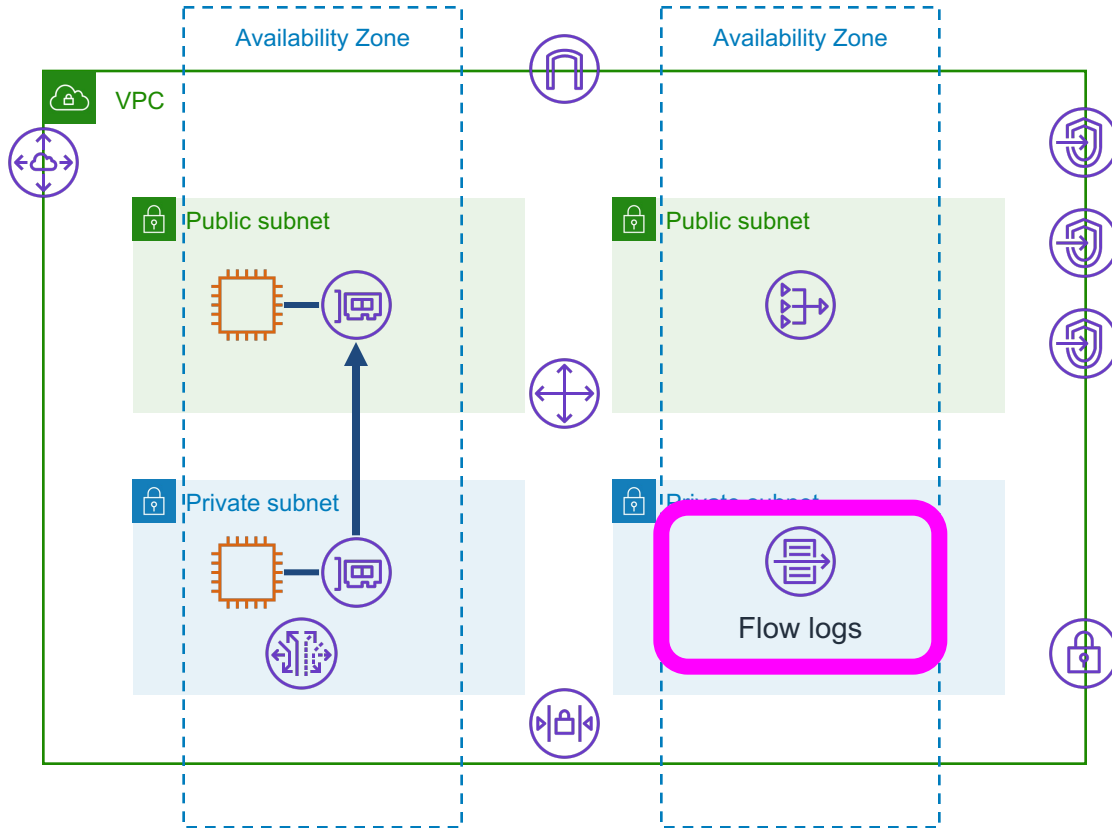
Transit Gateway Attachments are charged hourly and for traffic throughput, and can be more expensive than other options

Charged VPC Network Resources



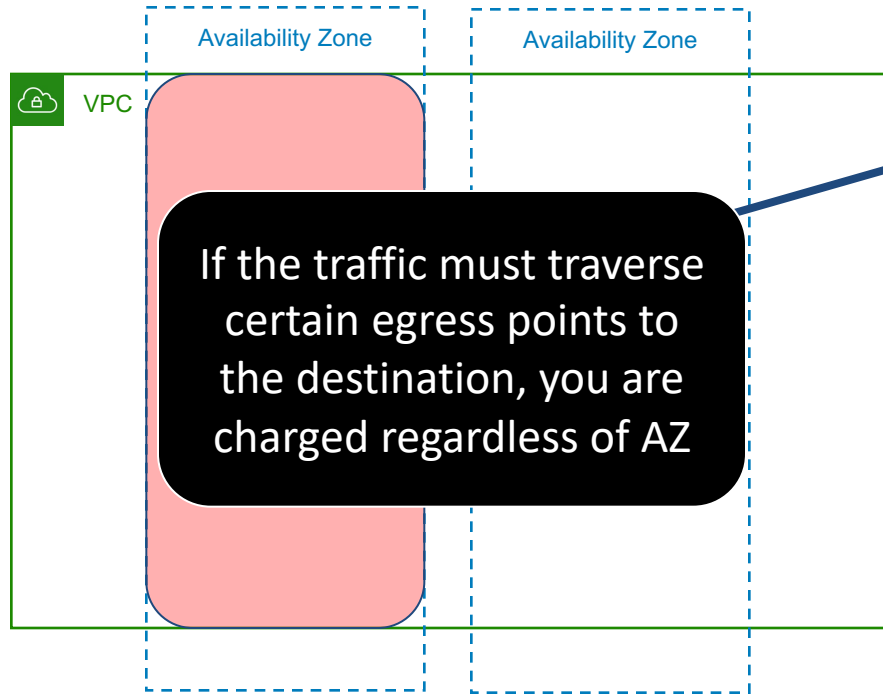
Traffic Mirroring is charged hourly per ENI that has mirroring enabled

Charged VPC Network Resources



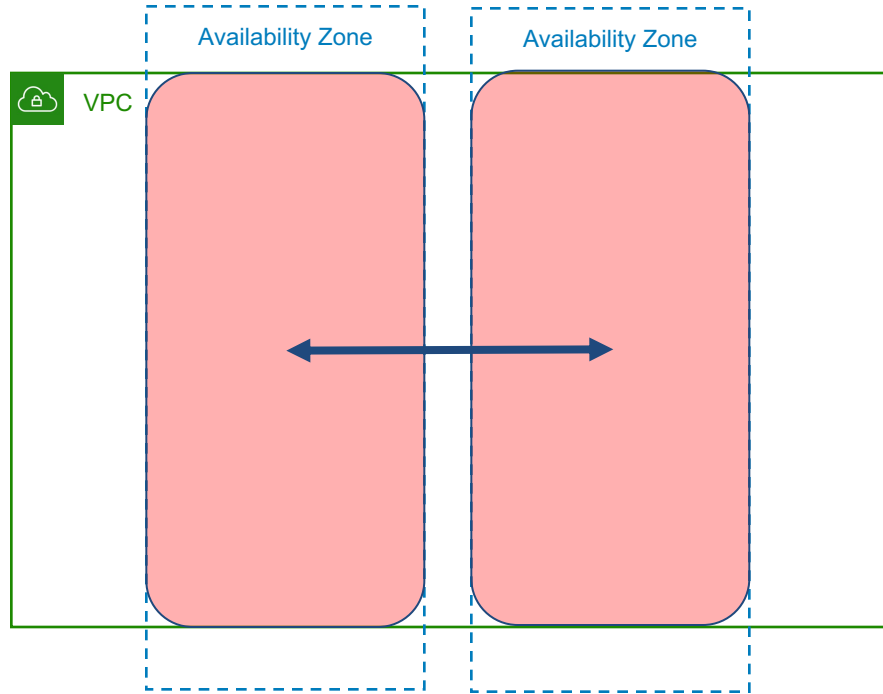
VPC Flow logs are charged according to the amount of traffic processed (and for log storage in the destination service)

Same-Region Traffic Charges



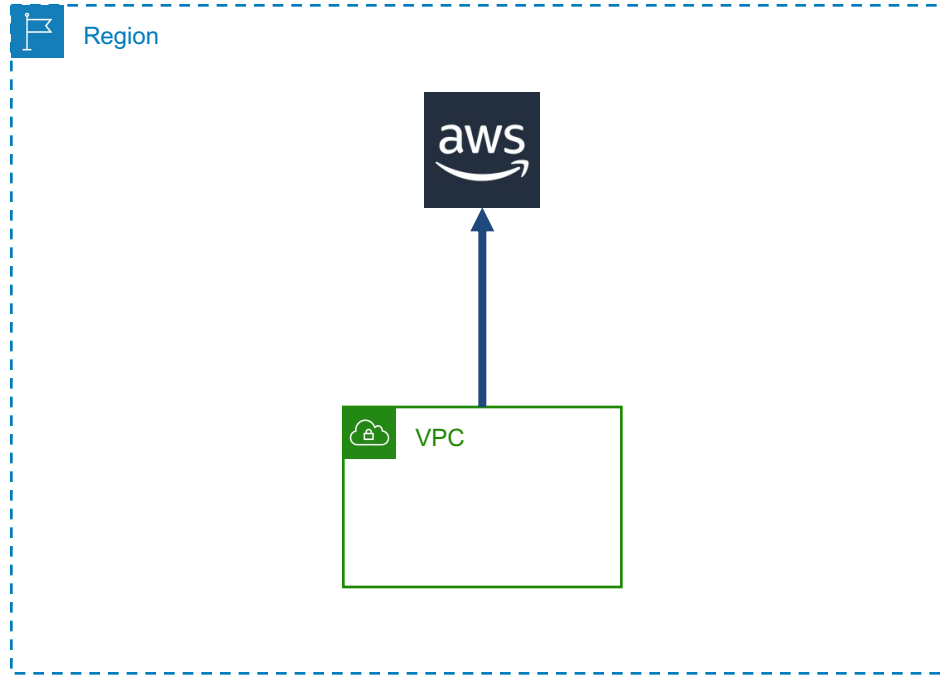
Any traffic with source and destination in here is free unless the destination uses the public IP

Same-Region Traffic Charges



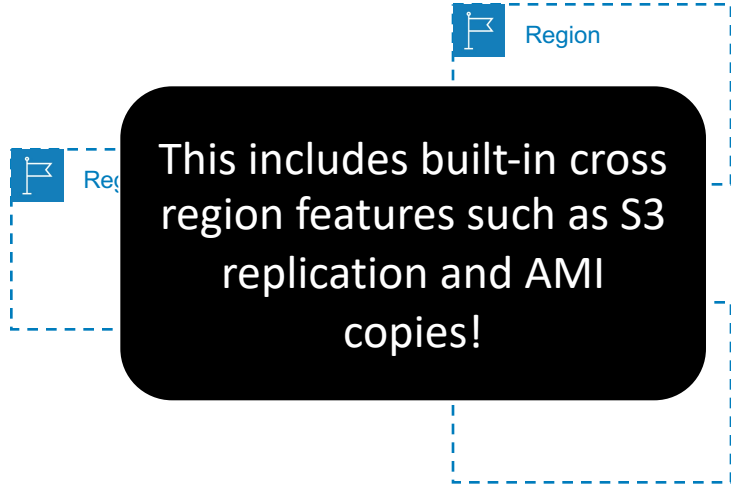
Any traffic with source and destination in different AZ is charged if the resource is AZ scoped

Same-Region Traffic Charges



Most same-region traffic from VPC to AWS services will be free, such as S3 bucket access, unless otherwise noted

Cross-Region Traffic Charges



All outbound cross-region traffic is charged, and there can be additional fees based on the gateway used

Cross-Region Traffic Charges

Internet

Some Internet outbound charges can be optimized, such as using CloudFront instead of S3 or ALB

All outbound Internet traffic is charged, and there can be additional fees based on the gateway used

Implement EC2 Optimizer



Wrap up and QA